TASK ORDER (TO)

47QFCA22F0029

Defense Counterintelligence and Security Agency (DCSA) One Information Technology (One IT)

in support of:

Department of Defense (DoD)

Awarded to:
Science Applications International Corporation (SAIC)
12010 Sunset Hills Road
Reston, VA 20190

Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

Mod Date:
August 2022

FEDSIM Project Number 47QFCA21Z1170

C.1 BACKGROUND

On behalf of the Department of Defense (DoD), the Defense Counterintelligence and Security Agency (DCSA) plays a vital role in safeguarding our nation's information. Under the National Industrial Security Program (NISP), DCSA is the designated oversight authority for the accreditation of classified facilities, information systems, and the insider threat program. This involves security oversight of more than 10,000 companies and approximately 13,000 facilities involved in classified work throughout the DoD and 31 Federal agencies. In addition, DCSA provides counterintelligence support to cleared personnel and programs to proactively identify threats and provide mitigations across approximately 167 field sites. DCSA services over 100 Federal entities and conducts approximately two million Background Investigations (BI) each year. DCSA also provides education, training, and certifications on best practices in technology and security for industry and Government personnel.

The DCSA Office of the Chief Information Officer (OCIO) is responsible for protecting and managing the critical data stored and exchanged in execution of the DCSA mission. This data includes Government-wide classified information for our nation's most important programs. While protecting this information, the OCIO ensures the availability of secure, reliable, and modern enterprise Information Technology (IT) services for DCSA's mobile field support staff and global customers accessing mission applications and DCSA IT networks. The One IT effort, overseen by the OCIO, will provide critical enterprise IT services and customer support at the Russell Knox Building (RKB) located in Quantico, VA; offices located in Boyers, Pennsylvania (PA) and around Fort Meade, Maryland (MD); and other remote locations within the Continental United States (CONUS). In addition, DCSA One IT will support nationally accredited training centers that provide security training, education, and certification products and services for security professionals across the Federal Government and industry.

C.1.1 PURPOSE

The purpose of the DCSA One IT effort is to acquire an enterprise IT solution that delivers highly secured and adaptable IT infrastructure, provides customer support, and cutting-edge technologies that support operations and advance the DCSA mission. Inherent to this purpose is the objective to create a more collaborative, integrated, transparent, predictable, and measurable organization under a single IT environment (i.e., One IT).

C.1.2 AGENCY MISSION

DCSA is the security agency in the Federal Government dedicated to protecting America's trusted workforce and trusted workspaces, real or virtual. DCSA joins two essential missions: Personnel Vetting and Critical Technology Protection, supported by counterintelligence and training, education, and certification functions.

DCSA's Personnel Vetting mission delivers efficient and effective BI, continuous vetting, and adjudications to safeguard the integrity and trustworthiness of the Federal and contractor workforce. DCSA conducts BI for 95 percent of the Federal Government, including 105 departments and agencies. Additionally, DCSA adjudicates 70 percent of the Federal Government's adjudicative determinations.

DCSA's Critical Technology Protection mission provides oversight to approximately 10,000 cleared companies under the NISP, ensuring that the sensitive and classified U.S. Government information it is entrusted with and the critical technologies it develops are properly protected. DCSA ensures that companies are adequately protecting their facilities, personnel, and associated IT systems from attacks and vulnerabilities.

DCSA's Counterintelligence supports both the Personnel Vetting and Critical Technology Protection missions to identify and stop attempts by our nation's adversaries—foreign and domestic—to steal sensitive national security information and technologies, keeping U.S. Government leaders and stakeholders informed of these threats. DCSA also has nationally accredited training centers that provide security training, education, and certification products and services for security professionals across the Federal Government and industry.

C.2 SCOPE

The contractor shall support DCSA to provide enterprise-wide IT services including architecture, engineering, enterprise operations, and National Industrial Security Programs (NISP) National Industrial Security Systems (NISS) applications and hardware support, and related IT services to support DCSA's centralized IT solution requirements.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

All information concerning the current DCSA IT/Network Environment is provided as a part of the DCSA One IT Reading Room, which is available upon request. Below are a few highlighted areas of current DCSA environments:

a. DCSA's network infrastructure consists of non-virtual and virtual systems in multiple DCSA enclaves, data centers, regional and field offices, and in the Amazon Web Service (AWS) Govcloud environments.

b. DCSA's enclaves include: Pre-Production, Production, Non-classified Internet Protocol Router Network (NIPRNet), Secret Internet protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communication System (JWICS), and DCSA's multiple cloud instances.

c. DCSA's datacenters supported by this TO are located in RKB Quantico, VA; Fort (Ft.) Meade, MD; Boyers, PA; Seaside, California (CA); Farmers Branch, Texas (TX); and Phoenix, Arizona (AZ) (anticipated in Calendar Year (CY) 2022).

d. For Web Content, DCSA currently uses Defense Media Activity Platform; however, the contractor may be required to support the implementation of other new technology solutions/platforms within DCSA's current and future environments.

e. The following technologies are required to support DCSA's IT environment for this work: Adobe Creative Suite, Adobe Creative Cloud – Dreamweaver, and other Adobe specialized tools, Microsoft (MS) Office Suite, Splunk, Oracle, SQL Server, Solar Winds, ServiceNow, MySQL, Visual Studio, Windows Operating System (OS), and any other web solution technology approved by DCSA. Additionally, DCSA is migrating to DoD Office 365 environment as part of the DISA tenant.

f. For SharePoint, DCSA currently uses the DoD/Defense Information Systems Agency (DISA), Enterprise Portal Services; however, the contractor may be required to support

the implementation of other new technology solutions/platforms within DCSA's current and future environments.

g. DCSA plans to migrate from Remedy to ServiceNow. The Service Now modules that DCSA will utilize are: IT Business Management (ITBM), IT Service Management (ITSM), Case Management, and Project Portfolio Management (PPM). It is anticipated that this migration will be complete prior to TOA; however, there is a chance that some migration may take place during the period of performance of this TO.

h. DCSA supports three training facilities at the Ft. Meade, MD; Slippery Rock, PA; and Ft. Jackson, South Carolina (SC). This support may expand to any area covered under the scope of this TO, including but not limited to the Center for Development of Security Excellence (CDSE), National Training Center (NTC), National Center for Credibility Assessment (NCCA).

i. The contractor shall be responsible for managing Data Center East (DCE) networks (comprised of NIPR, SIPR, and JWICS) and Data Center West (DCW) (NIPR only) (anticipated to relocate to Boyers, PA; Ft. Meade, MD; and RKB in CY 2021), and all associated infrastructure. DCE is also comprised of North Atlantic Treaty Organization (NATO), Insider Threat internal, and a Federal Bureau of Investigations (FBI) networks, for which the contractor shall only be responsible for managing network access connections.

j. It is anticipated by the time TO performance begins, DCSA will have transitioned approximately 350 Headquarters (HQ) users on NIPR and 650 HQ and Field users on SIPR to Virtual Desktop Infrastructure (VDI).

k. DCSA plans to move its existing JWICS platform to the common operating environment platform provided by the National Geospatial-Intelligence Agency (NGA) and the Defense Intelligence Agency (DIA). Some organizations within DCSA have already completed this migration (e.g., NCCA and Central Adjudication Facility) and all DCSA organizations should be transitioned within the next 12 to 18 months.

C.4 OBJECTIVE

The objective of the One IT effort is to provide DCSA with an enterprise IT solution that delivers highly secured and adaptable IT infrastructure, outstanding customer support, and cutting-edge technologies to support operations and advance the DCSA mission. The overarching objective for the TO is to have improvements to processes that will drive collaboration, integration, and transparency to achieve operational efficiencies. The contractor shall be responsible for delivering highly specialized expertise to meet these objectives. Other goals for this effort include, but are not limited to, providing:

a. Opportunities for quickly adopting cutting edge technologies and best practices to improve the overall IT environment.
b. Improvements to generate measurable standards for DCSA as it evolves to an enterprise IT environment.
c. Improvements/opportunities to integrate data and systems with the DCSA Integrated Operational Dashboard (IOD) in accordance with **TO Section C.5.2.3.5.**
d. Improvements to IT governance and information sharing using best practices.

e. Improvements to providing enterprise customer support.
f. Cost saving/cost avoidance measures.
g. Improvements to quality control efforts.

C.5 TASKS

a. Task 1 – Program Management
b. Task 2 – Information Technology (IT) Management Services
c. Task 3 – Architecture and Engineering (A&E)
d. Task 4 – Enterprise Operations
e. Task 5 – Program Executive Office (PEO) Support
f. Task 6 – NISP National Industrial Security Systems (NISS) Services
g. Task 7 – Tools/Asset Management Support
h. Task 8 – Surge Support (Optional)

C.5.1 TASK 1 – PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to oversee the execution of the requirements identified in this Performance Work Statement (PWS). The contractor shall identify a Program Manager (PM) by name who shall provide high-quality leadership, management, direction, administration, and quality assurance over the execution of this TO. The PM shall create, manage, and process all deliverables to support business operations to include, but not limited to, financial tracking and reporting TO metrics. The contractor shall create and implement processes to ensure compliance over the execution of the requirements and reporting of and expeditious resolution of any contractual issues that may arise during its implementation or execution. The contractor shall utilize industry best practices identified in Project Management Body of Knowledge (PMBOK).

Program Management also includes, but is not limited to, Customer Relationship Management (CRM), customer preference customization, and initiating services. The contractor shall manage all aspects of the CRM process, including planning, scheduling, and control activities involved with service delivery for the entire contract. The contractor shall facilitate and coordinate customer (i.e., DCSA's) interactions across multiple communication channels and business lines (e.g., real time chat, instant messaging, audio/video conferencing). The contractor shall customize customer preferences relative to interface requirements and information delivery mechanisms (e.g., presentations, personalization, alerts, and notifications).

C.5.1.1 SUBTASK 1-ACCOUNTING FOR SERVICE CONTRACT REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the DCSA. The contractor shall completely fill in all required data fields using the following web address: http://www.sam.gov.

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported No Later Than (NLT) October 31

of each calendar year. Contractors may direct questions to the support desk at: http://www.sam.gov.

C.5.1.2 SUBTASK 2 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government. The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting shall provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include the contractor's Key Personnel, the DCSA Technical Point of Contact (TPOC), other relevant Government personnel, the FEDSIM CO, and the FEDSIM COR.

At least three days prior to the Project Kick-Off Meeting, the contractor shall provide a **Project Kick-Off Meeting Agenda (Section F, Deliverable 01)** for review and approval by the FEDSIM COR and the DCSA TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of Contact (POCs) for all parties.
b. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
c. Project Staffing Plan (PSP) and status.
d. Transition-In Plan (in accordance with **TO Section C.5.1.8**) and discussion.
e. Security discussion and requirements (i.e., building access, badges, and Common Access Cards (CACs)).
f. Invoicing considerations.
g. Baseline Quality Management Plan (QMP) **(**in accordance with **TO Section C.5.1.7**).

The Government will provide the contractor with the number of Government participants for the Project Kick-Off Meeting, and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a **Project Kick-Off Meeting Minutes Report (Section F, Deliverable 02)**, documenting the Project Kick-Off Meeting discussion and capturing any action items.

C.5.1.3 SUBTASK 3 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an **MSR (Section J, Attachment F) (Section F, Deliverable 03)**. The **MSR** is a sample and not a designated template. The contractor may develop a format to be approved by the Government. The MSR shall include the following:

a. Activities during reporting period, by task (include on-going activities, new activities, and activities completed, and progress to date on all above-mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (e.g., security clearance and executed Non-Disclosure Agreements (NDAs)).

d. Government actions required for the contractor to execute specific tasks. Net results of Government action or inaction.
e. Schedule (show major tasks and projects, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach Trip Reports (**TO Section C.5.1.6**) to the MSR for reporting period).
g. Accumulated invoiced cost and incurred cost for each CLIN up to the previous month.
h. Projected cost of each CLIN and Task for the current month.

C.5.1.4 SUBTASK 4 – CONVENE TECHNICAL STATUS MEETINGS

The contractor shall develop a meeting battle rhythm schedule, in coordination with the DCSA TPOC, that ensures appropriate technical oversight of all tasks supported under this order.

At a minimum, the contractor shall provide the following technical status meetings:

a. Weekly stand-up briefing for senior leadership.
b. Daily IT Service Desk (SD) ticket reporting.
c. Daily technical status briefing (including offline/online systems, issues, and other status updates).

The contractor PM shall convene a monthly Technical Status Meeting onsite at DCSA HQ with the DCSA TPOC, FEDSIM COR, and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR (**Section F, Deliverable 04 Technical Status Meeting Minutes**).

C.5.1.5 SUBTASK 5 – PREPARE AND UPDATE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a **PMP** and shall provide it to the Government (**Section F, Deliverable 05**). The PMP must include the contractor's overall management approach and plan to manage, track, and evaluate the TO performance, including a description of the contractor's approach to quality management in the context of DCSA One IT, and of how the contractor shall successfully implement and tailor a comprehensive quality management strategy that will enable the contractor to maintain minimum quality standards for all functions performed under this contract. The contractor's PMP must fully address typical management challenges that exist, and mitigating action plans to be implemented by the contractor for operating and managing a TO similar in size, scope, and complexity of DCSA One IT. The PMP must tie to the Integrated Master Schedule (IMS) and include milestones where Government information/activity is required and timeline dependencies for subsequent contractor activities. The PMP shall describe the contractor's approach to enterprise communications, including processes, procedures, communication approach, and other rules of engagement between the contractor, DCSA divisions, and FEDSIM.

At a minimum the PMP shall:

a. Describe the proposed management approach.

b. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this TO.
d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
e. Describe in detail the contractor's approach to risk management under this TO.
f. Describe in detail the contractor's approach to communications, including processes, procedures, format, and other rules of engagement between the contractor and the Government.
g. Include the contractor's QMP.
h. Include **TO IMS** to identify the status of all TO projects (**Section F, Deliverable 06**).

The PMP is an evolutionary document that shall be updated annually at a minimum and as project changes occur. The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.6 SUBTASK 6 – PREPARE TRIP REPORTS

The Government will identify the need for a **Trip Report** when the request for travel is submitted (**Section F, Deliverable 07**). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, **Trip Reports** shall be prepared with the template information provided in **Section J, Attachment G (Trip Report Template)**.

C.5.1.7 SUBTASK 7 – PROVIDE QUALITY MANAGEMENT

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor shall provide a **QMP** and maintain and update it as changes in the program processes are identified **(Section F, Deliverable 08**). The contractor's QMP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The contractor shall fully discuss its validation processes and procedures for providing high-quality performance for each task area and subordinate tasks. The QMP shall describe how the appropriate methodology integrates with the Government's requirements. The Government's **Quality Assurance Surveillance Plan (QASP)** provided in **Section J, Attachment P**.

C.5.1.8 SUBTASK 8 – TRANSITION-IN

The contractor shall provide a **Transition-In Plan (Section F, Deliverable 09)** as required in Section F. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall implement its Transition-In Plan NLT the Project Start (PS) date, and all transition activities shall be completed by 60 calendar days after PS.

At a minimum, the contractor's Plan shall include a plan to maintain a continuity of services, ensure the smooth transfer of knowledge on ongoing projects, and onboard staff within the timeframe identified. The contractor's Plan shall identify risks and mitigation strategies to ensure there is no degradation of services.

C.5.1.9 SUBTASK 9 – TRANSITION-OUT

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a **Transition-Out Plan** within six months of PS (**Section F, Deliverable 10)**. The contractor shall review and update the Transition-Out Plan in accordance with the specifications in **Sections E and F**. During transition the contractor shall provide support in a manner that ensures a timely and efficient transfer of work without any degradation of security. The contractor must identify, mitigate, and minimize transition risks.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor/Government personnel to transfer knowledge regarding the following:

a. Project management processes.
b. POCs.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel roles and responsibilities.
g. Schedules and milestones.
h. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

C.5.1.10 SUBTASK 10 – DEVELOP AND MAINTAIN A TASK ORDER (TO) PORTAL

The contractor shall develop, manage, maintain, and host an unclassified TO portal that Government-approved contractor personnel and Government personnel can access worldwide via unique user identification and password. The TO portal shall not be CAC enabled but shall be a cloud-based solution available to users with a .mil and a .gov account. The contractor shall provide a multi-factor authentication process with a TO Portal Strategy and identify this strategy in its proposal. The contractor shall provide the FEDSIM COR and the DCSA TPOC with the **TO Portal Strategy/Solution (Section F, Deliverable 11)**. The proposed dashboard solutions may leverage existing tools or new technology. The solutions shall meet all DoD policies and mandates for system security, including the Authority to Operate (ATO). A discussion of the capabilities of the TO portal will occur at the Project Kick-Off Meeting. Once the FEDSIM COR has provided the contractor approval of the TO Portal Strategy, the contractor shall develop and implement the approved solution.

The objective of the TO portal is to introduce efficiencies, ensure coordinated service delivery, and create automated capabilities that requires little to no manual effort. The Government seeks improvements for managing workflow processes. Over the life of the TO, the contractor shall continually identify opportunities to enhance the dashboards with new integration and capabilities.

At a minimum it is required that the TO Portal Solution shall have the following:

a. Serve as a repository for all unclassified TO deliverables.
b. Dashboards that provide program management and financial views for the purpose of monitoring enterprise health, tracking metrics, and providing operational reports on a near real-time basis.
c. Provide financial forecasting and dashboard views providing a status of the financial health of the TO (in accordance with **Section C.5.1.11**).
d. The portal shall also be capable of Role-Based Access Control (RBAC) to limit access to the various workflows.

C.5.1.11 SUBTASK 11 – FINANCIAL FORECASTING

The contractor shall work with the FEDSIM COR and the DCSA TPOC to track and create a financial forecast for each TO period of performance that details the anticipated monthly costs for labor (broken down to the task and subtask level), travel, tools, and ODCs. The contractor shall set the baseline at the start of each TO period of performance and update the forecasts monthly, at a minimum, as costs are incurred, or requirements change.

The contractor shall present a proposed format for the **Financial Forecast (Section F, Deliverable 12)** at the Project Kick-Off Meeting for FEDSIM COR and DCSA TPOC approval. Once approved, the contractor shall use the Government-approved format.

C.5.1.12 SUBTASK 12 – MANPOWER REPORTING

The contractor shall provide a monthly **Manpower Report (Section F, Deliverable 13)** under the TO. The Manpower Report shall be provided in MS Excel format and easily sorted to identify manpower resources at the contract-level delineated by DCSA office. This report shall furnish a list of detailed information for all personnel supporting all tasks. The following information is required:

a. Employee full name (last name, first name, middle initial).
b. TO assigned.
c. Labor category/position name.
d. Billable CLIN.
e. Position status (e.g., vacant, onboard, pending onboarding, dissociated).
f. Organizational information
    1. Company of employment.
    2. Prime/Subcontractor status.
    3. Organization supported at a division level (if more than one, include column for the percent of time allocation for each effort).
    4. Project(s) supported.

5. Work location.
6. Work schedule (e.g., Monday through Friday, 9:00 a.m. to 5:00 p.m. Eastern Time (ET))
7. Approved telework status (e.g., approved full time, approved situational, pending, not allowed).
8. DoD email.

g. Clearance information (if applicable)
   1. Clearance level.
   2. BI status.

h. Date disassociated from order (applicable to contractor employees no longer supporting the order).

i. Badge information:
   1. Badge number.
   2. Badge expiration date.
   3. Facility where badge was issued.
   4. Date badge returned to Government (applicable to contractor employees no longer supporting the contract).

j. Training completion dates including, but not limited to, the following:
   1. Cyber Security Awareness.
   2. Annual Privacy Awareness.
   3. Other training as mandated.

C.5.1.13 SUBTASK 13 – ONBOARDING/OFFBOARDING CHECKLISTS/PROCESSES

The contractor shall create and maintain a standardized process and develop and deliver an **Onboarding/Offboarding Checklist (Section F, Deliverable 14).** The processes shall be used for OCIO contracts and aim to ensure the smooth in processing and offboarding of personnel across the office. The checklist processes at a minimum shall include, receipt of Government-Furnished Property (GFP) and Government-Furnished Equipment (GFE) equipment, a "how to" to create credentials, Badge request process for both CAC and building/site access, provisioning/deprovisioning email accounts, account creation process for JWICS, NIPR, SIPR accounts, administrative access accounts (e.g., elevated accounts for administering other users, servers), and other accounts as necessary. Additionally, the contractor shall create and deliver out-processing processes, including a process to instantly disable accounts, and return GFP/GFE.

C.5.2 TASK 2 – INFORMATION TECHNOLOGY (IT) MANAGEMENT SERVICES

C.5.2.1 SUBTASK 1 – INFORMATION TECHNOLOGY (IT) SERVICE STRATEGY AND INNOVATION

The contractor shall provide strategic IT management guidance and planning across DCSA to apply innovative services and utilize optimization and performance delivery across the enterprise. The contractor shall assist the Government with development of transformational strategic goals by utilizing industry best practices, enhancing processes/solutions, proposing alternatives, and highlighting potential risks, all in pursuit of optimizing the enterprise-wide IT service delivery across DCSA. The contractor shall facilitate strategic communication design,

implementation strategies, and stakeholder engagement in accordance with **TO Section C.5.2.3.3**. The contractor shall provide recommendations on innovative design, development, implementation, and cultivation of IT service management as a strategic asset and not only an organizational capability. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report (**Section F, Deliverable 144**, **Activity Report**).

The contractor shall provide IT management guidance regarding infrastructure Architect and Engineering (A&E) support services to align with DCSA's enterprise capabilities to the vision and direction of the overall OCIO strategic priorities. This will ensure the One IT service delivery can effectively support the current and future requirements of mission and business portfolios. The contractor shall:

a. Assist the Government with developing a highly motivated and creative organization that leverages the diverse skill sets of the people, innovative tools, and collaborative culture to work productively from anywhere.
b. Establish a model to enable the rapid delivery of high-quality IT products and services that exceed customer expectations.
c. Improve the IT environment through the maturation of IT governance to drive clear understanding of roles and responsibilities with increased accountability.
d. Centralize IT capabilities to accomplish essential business functions and enable critical missions across the agency.
e. Provide strategies to modernize IT systems to improve mission effectiveness, create fiscal efficiencies, and provide the right level of security to our systems and information. Research state-of-the-art technology for potential DCSA usage and develop recommendations for new and cutting-edge technologies.
f. Provide strategies to improve onboarding and offboarding processes to ensure a timely, secure, and user-friendly experience.
g. Provide strategies for planning, designing, conducting, coordinating, and advising on projects and programs of broad scope and unusual complexity involving systems engineering/computer science and technical integration concepts in network design and optimization areas.
h. Perform DCSA systems analysis and apply engineering/computer science concepts in support of technical projects.
i. Participate with and provide expertise to Government Program Executive Officers (PEOs), program and project managers, senior scientists, hardware and software developers, technical staff, and policy makers across DCSA.
j. Provide technical guidance, advisory support, and assistance on an entire project or major phases for broad and varied operations.
k. Provide technical expertise, advice, and guidance for preparation of DCSA infrastructure systems plans, designs, and specifications for DCSA programs and projects in the network optimization and hardening areas. Assist the Government in performing complex studies/evaluations.
l. Perform critical analysis concerning engineering/computer science and implementation of cloud infrastructure. Consider all applicable policy, design criteria, and approved cloud architectures. Incorporate mission system survivability, redundancy, and technical

performance for optimum defensibility of DCSA systems and critical infrastructure. Work closely with DCSA program/project managers to facilitate required changes to new (research and development) and ongoing (acquisition stage) programs/projects. Participate in ongoing technical teams involved with the engineering, computer science, implementation, and test of these programs, projects, and technologies.

As part of the Innovation Services, the contractor shall support A&E (in accordance with **TO Section C.5.3**) to introduce emerging technologies and infuse innovation into program solutions and operations when approved by DCSA. The engineering function shall support the full range of infrastructure engineering design, enterprise architecture standards, prototyping, and integration, including, but not limited to, concept development, planning, requirements definition and analysis, systems design, system integration into the current environment, and deployment, including all necessary onboarding and approvals from higher HQs or any Department or agency overriding authority. The A&E function shall ensure a smooth hand-off to Enterprise Operations (in accordance with **TO Section C.5.4**) for implementation. Example of contractor's functions include, but are not limited to:

a. Open Systems Interconnection (OSI) Model L1-7 design, analysis, engineering, design, installation, and documentation.
b. SecureView.
c. Enhanced Virtual Desktop Infrastructure (eVDI).
d. Big data analytics.
e. Mobility management.
f. Active/Active datacenters.
g. Zero trust.
h. Disaster Recovery (DR) and Continuity of Operations (COOP) design, architecture, and capability.
i. Data Center as-is documentation, design, and analysis.
j. Maintain a lab environment (separate from pre-production environment) on DCSA systems for testing and piloting new and enhanced technologies.
k. Develop and implement service design principles, practices, and methodologies to convert strategic objectives into actionable and supportable portfolios of well-integrated IT services and service assets.
l. Develop and maintain a holistic forward-looking **IT Optimization and Transformation Plan (Section F, Deliverable 15)** to incrementally transform services and infrastructure, where emerging technologies provide a more resilient and agile business environment.
m. Perform analyses of operations, network sensor performance and configuration, and network assessment.
n. Develop and document incident response and recovery procedures, road maps to implement data loss prevention strategies, two factor authentication, digital signatures, email encryption, endpoint encryption, access management solutions, file and folder encryption, network segmentation, and anomaly detection.
o. Provide research, analyses, and recommendations for defining Concept of Operations (CONOPS), techniques, and procedures that embed cyber threat detection and signature analyses processes in network sensors and operations.

C.5.2.2 SUBTASK 2 – USER EXPERIENCE

The contractor shall provide support to DCSA's User Experience Division. The User Experience Division serves as OCIO's strategic communications partner to improve overall workforce productivity, create a positive OCIO presence, and instill a sense of trust among the user community. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report (**Section F, Deliverable 144, Activity Report**). The contractor shall deliver the below listed tasks using appropriate MS Office Suite products (e.g., emails, Excel, Power Point presentations) on a specific frequency or on an as needed basis

The contractor shall:

a. Work with Government personnel to establish, translate, and manage operational and mission requirements for DCSA.
    i. Interview stakeholders, gather requirements, analyze requirements, and build presentations with courses of action, Plan of Actions and Milestones (POA&M) objectives, risks mitigation objectives, project status, and decision points.
    ii. Perform needs analysis to determine opportunities for new and improved business process solutions using the ticket management system (ServiceNow) application capabilities. Document report via Information Technology Capability Request (ITCR) forms.
b. Gather feedback on ITCR customer satisfaction and internal service performance to foster continual improvement.
c. Assist the Government with initiating, tracking, consolidating, and briefing stakeholder communications to align and manage expectations with agency strategy and priorities.
d. Assist the Government with the development of communication/briefing products including, but not limited to: Newsletters, Roadshows, Operational Training Events, Town Halls (Weekly/Monthly/Quarterly), and Operational Briefs.
e. Assist the Government with the production and dissemination of high-quality data and survey products on performance of OCIO products and services to effectively measure and monitor areas of improvement.
f. Provide expert technical advice, guidance, and recommendations to management and other technical specialists on critical IT issues.
g. Analyze trends and measure potential impacts to DCSA, ongoing IT initiatives, and the Agency's mission.
h. Provide troubleshooting advice and lessons learned and mitigate future IT issues.
i. Assist the Government with the coordination and performance of technical assessments and evaluations of requirements and acquisition requests submitted by technical and program stakeholders to ensure conformance with approved plans, program objectives, and policies as well as efficient use of assets.
j. Assist the Government with managing the internal relationship with IT process owners supporting the service and assist the Government with defining the terms of Operating Level Agreements (OLAs).
k. Develop and document supply chain risks for critical system elements and IT systems status communications (e.g., impacts, outages, push updates).

l. Perform Division administrative services including, but not limited to, calendar maintenance, meeting management, briefings.
m. Maintain an advanced level of expertise in MS Office Suite and virtual collaboration tools (e.g., MS Teams, ZoomGov, Adobe Connect).
n. Assist Division leadership with the development and maintenance of three to five-year **Strategic Vision, Goals, and Briefs (Section F, Deliverable 16)**.

C.5.2.3 SUBTASK 3 – INFORMATION TECHNOLOGY (IT) MANAGEMENT CONTROLS

The contractor shall assist DCSA management with the development of IT management controls and identification of systems that are required by agencies to evaluate, manage, and monitor program performance relative to IT initiatives. The contractor shall assist the Government with the development of IT policies, guidelines, and standards to facilitate implementation of Federal laws and regulations. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report (**Section F, Deliverable 144, Activity Report**). These services shall include, but are not limited to:

a. DoD/DCSA, program, and project-level performance plans for IT initiatives.
b. Assist the Government with recommending performance measures to support evaluation and reporting requirements for IT initiatives in compliance with DoD/DCSA Performance Reference Model (PRM) standards.
c. Draft performance measures to support evaluation and reporting requirements for IT initiatives in compliance with DoD/DCSA PRM standards.
d. Support the development, implementation, and maintenance of systems to support agencies' IT regulatory development, compliance, and enforcement activities.
e. Monitor, inspect, or audit IT-regulated activities to ensure compliance.

C.5.2.3.1 INFORMATION TECHNOLOGY (IT) OPERATIONAL PROJECT MANAGEMENT

The contractor shall provide IT project management support as required for task projects under this TO. The contractor shall develop an **IT Operational Project Management Plan (Section F, Deliverable 17)** for all major IT projects (existing and new) as required by the FEDSIM COR, in coordination with the DCSA TPOC. The IT Operational Project Management Plan shall include all anticipated project phases, deliverables, staffing plan, schedule and milestones, costs, and risks. The contractor shall brief the IT Operational Project Plan to the Government as an **IT Operational Project Briefings (Section F, Deliverable 18)** on all active projects.

C.5.2.3.2 AFTER ACTION REPORT (AAR) AND ROOT CAUSE ANALYSIS (RCA)

The contractor shall provide an **After Action Report (AAR) (Section F, Deliverable 19)** following a problem or situation that has occurred in the past, is underway, or could happen in the future. AARs shall report situation–response interactions, analyze critical procedures, and identify problems, if known, and propose adjustments and recommendations. The Government may convene review meetings as needed. If the situation merits, the contractor shall provide a **Root Cause Analysis (RCA) (Section F, Deliverable 20)**. RCAs shall be reported following major outages and issues (i.e., Priority 1) that occur during performance of the TO.

C.5.2.3.3 STRATEGIC COMMUNICATIONS PLAN AND IMPLEMENTATION

The contractor shall work with DCSA/CIO management to coordinate and develop, deliver, and implement a strategic communications strategy for the office with an emphasis on DCSA's values of people and culture. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report)**. The contractor shall:

a. Assist the Government on executive-level and working-level teams through vision and strategy development, change management, and team building processes with an emphasis on Lean techniques and Agile methodologies.
b. Integrate a blend of visual facilitation techniques and design thinking methods to help organizations deliver outcome-focused goals and strategies, prototypes and new ideas, and product delivery and maturation plans.
c. Facilitate strategic communication design, implementation strategies, and stakeholder engagement (in accordance with **TO** Section **C.5.2.1**).
d. Produce graphic recording and digital recording (hand-drawn posters and digital drawings) in real-time during multi-hour and multi-day meetings to artistically capture and summarize key discussion and decision points.
e. Provide graphic design, white board video development, and data visualization to shape concepts into communication products.

The contractor shall develop and deliver a **Strategic Communications Plan (Section F, Deliverable 21)**. The contractor's strategic communications plan must define communications goals and objectives, target audiences and stakeholders, a communications strategy, as well as an implementation plan. After gaining approval from the Government, the contractor shall activate and coordinate implementation of the strategic communications plan. The contractor shall conduct periodic assessments and report the results to DCSA management and update the plan accordingly.

C.5.2.3.4 DAILY STATUS REPORT

The contractor shall prepare and deliver a **Daily Status Report (DSR) (Section F, Deliverable 22)**. The contractor shall create an automated process and integrate into the IOD **(Section C.5.2.3.5)**. The contractor shall compile technical information from all offices including, but not limited to, Central Adjudication Facility, Legacy BI, and Operations and send to leadership on a daily basis in a format determined by DCSA. The contractor shall prepare the report in coordination with the Government. The DSR shall provide a summary of the notable items from the morning's status meeting and overall operations status of DCSA by location.

C.5.2.3.5 DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA) INTEGRATED OPERATIONAL DASHBOARDS (IOD)

The contractor shall develop a dashboard solution that provides IT operational views, monitors enterprise health, tracks metrics, and reports on a real-time basis (**Section F, Deliverable 23-IOD Solution and Project Plan**). The contractor may use available tools such as Splunk and may be required to integrate information from ServiceNow in the future. The dashboard shall integrate seamlessly and securely with enterprise systems, applications, and data. The dashboard will host all NIPR enclave information. The objective of the integration is to create automated

capabilities that require little to no manual effort. The proposed dashboard solution may leverage existing tools or new technology. The proposed solution shall meet all DoD policies and mandates for system security, including the ATO. Over the life of the TO, the contractor shall continually identify opportunities to enhance the dashboard with new integration and capabilities.

The solution for NIPR shall include the following capabilities:

a. Ability to monitor real-time enterprise health and status of systems and services.
b. Integrated views that provide a common operational picture or "single pain of glass."
c. Operational indicators and updates that provide relevant and actionable intelligence.
d. Real-time data collection and metrics.
e. Active link, two-way communication.
f. Data analytics.
g. Automated report generation.
h. User based views (e.g., executive-level, operator-level).
i. Ability to view the status of POA&Ms.
j. A list of upcoming hardware/software maintenance renewals (within 90 days of expiration).

The contractor shall update the IOD Project Plan with further details on the scope, milestones, schedule, and an integration plan that achieves IOC (**Section F, Deliverable 23-IOD Solution and Project Plan)**. The Government will provide comments and/or approval IOD Project Plan and the contractor shall finalize in accordance with the Government's comments.

C.5.2.3.6 INFORMATION TECHNOLOGY INTEGRATED MASTER PLAN (IT IMP) INFORMATION TECHNOLOGY INTEGRATED MASTER SCHEDULE (IT IMS)

The contractor shall develop and deliver an **IT IMP (Section F, Deliverable 24)** and an **IT IMS (Section F, Deliverable 25)** after TO award. The IT IMP and IT IMS shall follow the principles of the PMBOK and DoD guidelines for similar products. The IT IMP must include significant accomplishments encompassing all steps necessary to satisfy all TO objectives and requirements, manage all significant risks, and facilitate Government insight for each event. Significant accomplishments must be networked to show their logical relationships and that they flow logically from one to another. The IT IMP, and the supporting detailed schedules of the IT IMS, shall be used by the DCSA and contractor's team as the day-to-day tool for the planning, executing, and tracking program/TO technical, schedule, and cost status, including risk mitigation efforts and lessons learned. The IT IMS must include the contractor's current, best estimate of planned start and finished dates of all unfinished activities. Finished activities must include their actual start and finish dates.

C.5.2.3.7 TRAINING/KNOWLEDGE TRANSFER

The contractor shall plan, prepare, and provide training and internal knowledge transfer as well as the procurement/coordination/execution of commercially available training for all tasks covered under this task order. The contractor shall support the purchase of associated training for Government staff as required by this TO **(Section F, Deliverable 145, Training Procurement**

Report). The Government estimates that two-to-three training courses would be required per CY **(Section F, Deliverable 146, Training Execution Report)**.

C.5.2.3.8 STANDARD OPERATING PROCEDURES (SOPs)

The contractor shall develop and maintain a robust **IT SOPs (Section F, Deliverable 26**) for all tasks and subtasks within the TO and maintain the SOPs with in the TO Portal Solution (in accordance with **TO Section C.5.1.10**). SOPs shall be developed and maintained in line with industry best practices, current DoD guidelines, and updated to reflect process improvements. The contractor shall utilize these SOPs to facilitate knowledge transfer and train staff. The SOPs shall remain current and facilitate DCSA's management and monitoring activities surrounding core business operations. The contractor shall submit all SOPs and revisions to the Government for approval prior to implementation.

C.5.2.4 SUBTASK 4 – SOFTWARE LIFECYCLE MANAGEMENT (LCM)

Upon Government approval of the technical design documentation, the contractor shall perform Agile-based iterative development activities, which allow for frequent delivery of application changes. The contractor shall use industry best practices and methodologies when performing development. The contractor shall use baselined cost and schedule for assessment of planned versus actual performance. The contractor shall inform the Government of risks, impacts, and potential changes to the project scope, schedule, costs, and product quality.

The contractor shall:

a. Provide Risk Management and create and maintain a **Life Cycle Management Plan (LCMP) with Risk Register (Section F, Deliverable 27)** to include identified risks, qualitative analysis, triggers, and responses.
b. Provide **Software Meeting Agendas, Meeting Minutes, and Action Logs**, and Risk Registers in support of weekly status meetings (**Section F, Deliverable 28)**.
c. Escalate issues that arise during development to the Government with issue impact reports.
d. Develop Resource Breakdown Structure (RBS) that provides full visibility on resource allocation and schedules.
e. Provide documentation on development activities to address knowledge transfer with the Operations and Maintenance (O&M) team.

In addition, the contractor shall provide the following commonly known software lifecycle written products (reference example NISS Lifecycle Development Documentation (**Section F, Deliverable 123**)):

a. Software Code/Software Code Integration between systems.
b. Release Summary Report.
c. System Architecture/Design Documents with process flow diagrams.
d. Technical Requirements Documentation.
e. Requirements Traceability Matrix.
f. Network Typology.
g. Installation/User Guide.
h. Risk Management Framework (RMF) Compliance Documentation.

i. Deployment Plan.
j. Data Dictionary with Meta-data Mapping (Schema).

C.5.2.5 SUBTASK 5 – RISK MANAGEMENT FRAMEWORK (RMF) SUPPORT

The contractor shall comply with Department of Defense Instruction (DoDI) 8500, 8510, and RMF Knowledge Portal for Tier III level support specific to information systems owners and PM roles and responsibilities towards obtaining system authorization, assessments, and performing continuous monitoring for DCSA's systems, applications, network, and cloud services. This includes the six steps of RMF and step 0 delineated below. This will support the Assessment and Authorization (A&A) submission process for all specialized network systems, software, and hardware used on DCSA networks (enclaves – NIPR, SIPR, JWICS, Cloud) in accordance with applicable DoD policies.

The contractor shall provide all technical, engineering, application installation, and other implementation support services for maintaining and complying with the following Security requirements: Security Recommendation Guides (SRGs), Security Technical Implementation Guides (STIGs), Information Assurance Vulnerability Management (IAVM), various capability package requirements including, but not limited to: Mobile Access Capability Package (MACP), Data at Rest (DAR), and Multi-Site Connectivity as well as any other security policies applicable to the infrastructure components of the overall system solution. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report).**

The contractor shall ensure all baseline configurations across endpoints are done securely with STIG compliance in accordance with DoD mandates. Mobile Device Management (MDM), Unified Endpoint Management (UEM), and any Unified Capabilities (UC) infrastructure utilized shall be UC-approved and product list compliant. Mobile devices and MDM shall also be National Information Assurance Partnership (NIAP) certified per the appropriate protection profile.

DCSA follows the RMF for Federal Information Systems developed by the NIST with the goals of improving information security, strengthening the overall risk management process, and encouraging system reciprocity among Federal agencies.

The contractor shall support the Government's Technical Lead and Information System Owner (ISO) in completing the RMF process, including a preparatory step and six main steps, as follows:

a. RMF Step 0 – Prepare
    1. Register for Enterprise Mission Assurance Support Service (eMASS) accounts in order to upload documentation and provide updates to the ISO on the status of documentation.
    2. Support the Government Technical Lead and ISO with determining authorization boundaries.
    3. Support the Government Technical Lead and ISO with completing and signing the **IT Questionnaire (Section F, Deliverable 29)**.
    4. Support the Government Technical Lead and ISO with providing the initial artifacts for review including **RMF Hardware/Software Inventory (Section F, Deliverable**

30); **Detailed Architecture Diagram(s) (Section F, Deliverable 31)**; **CONOPS (Section F, Deliverable 32)**; **Ports, Protocols, and Services (PPS) (Section F, Deliverable 33)**; and running services/open sockets.

5. Support the Government Technical Lead and ISO with submitting tickets (within the enterprise ticket management system) requesting "Authorization Services."
6. Support the Information System Security Officer (ISSO)/Information System Security Manager (ISSM) with scheduling the "RMF Security onboarding meeting."

b. RMF Step 1 – Categorize

1. Support the Government Technical Lead and ISO with categorizing the system(s), identifying data types and impact values, identifying overlays, and completing **Categorization Level Agreements (CLA) (Section F, Deliverable 34)**.
2. Support the Government Technical Lead and ISO with completing documents such as, but not limited to; **Privacy Threshold Analysis (PTA)** and a **Privacy Impact Analysis (PIA) (Section F, Deliverable 35)** or **System of Record Notice (SORN) (Section F, Deliverable 36)**, as required.
3. Support the Government Technical Lead and ISO in registering the system(s) in the DCSA eMASS instance including system information, authorization information, assigned roles, detailed diagrams, architecture diagram/Network Topology, data flow (**Section F, Deliverable 37**, **eMASS Registration Documentation)**, hardware/software inventory import, PPS import, and the **Federal Information Security Management Act (FISMA) Information Form (Section F, Deliverable 38)**.
4. Support the Government Technical Lead and ISO with updating tickets (within the enterprise ticket management system) to verify that Step 1 tasks are complete.
5. Support the Government Technical Lead, ISO, ISSO, and ISSM by attending Categorization Review Meetings.

c. RMF Step 2 – Select

1. Support the Government Technical Lead and ISO with drafting **Security Controls and Overlays (Section F, Deliverable 39)**.
2. Support the Government Technical Lead and ISO with completing system registration in eMASS including system information, authorization information, FISMA, Business, and External Security Services.
3. Support the Government Technical Lead, ISO, and Cyber Architect with identifying **Common Controls documentation (Section F, Deliverable 40)**.
4. Support the Government Technical Lead, ISO, ISSO, ISSM, Information System Security Engineer (ISSE) with tailoring security controls.
5. Support the Government Technical Lead and ISO with developing **System-Level Continuous Monitoring (SLCM) Plan (Section F, Deliverable 41)**.
6. Support the Government Technical Lead and ISO with the completing **eMASS Security Control Implementation Plan(s) (Section F, Deliverable 42)**.
7. Draft **Systems Security Plan (SSP) Artifacts (Section F, Deliverable 43)**, including but not limited to: documents/artifacts required for the approval of the SSP: CLA, detailed architecture diagrams, revisions, or updates (**Section F, Deliverable 44, RMF SSP Artifacts**); hardware and software inventory and revisions or updates (;

Ports, Protocols, and Services Management (PPSM) spreadsheet, PTA/PIA, and **Memoranda of Agreement (MOAs)/Memoranda of Understanding (MOUs) (Section F, Deliverable 45)**.

8. Support the Government Technical Lead and ISO with verifying that all required SSP artifacts are uploaded in eMASS and submitted/ingested the SSP through the eMASS Package Approval Chain (PAC).
9. Support the Government Technical Lead, ISO, Cyber Architect, and Security Control Assessor Representative (SCAR) with reviewing the completeness of the **Security Assessment Plan (SAP) (Section F, Deliverable 46)**.
10. Support the Government Technical Lead and ISO with the coordination of Cyber Defense Operations to ensure the system(s) is registered for scanning and that tools are in place.
11. Support the Government Technical Lead and ISO with notifying ISSM, via the ticket management system, that all Step 2 tasks are complete.
12. Support the Government Technical Lead, ISO, ISSO, and ISSM by attending the ATP meetings.

d. RMF Step 3 – Implement (100 percent Self-Assessment)
   1. Support the Government Technical Lead and ISO with implementing control solutions consistent with DoD component cyber security architectures.
   2. Support the Government Technical Lead and ISO with beginning STIG/SCAG Self-Assessment, execute Assured Compliance Assessment Solution (ACAS) Scans, and complete **RMF Applicable Checklists (Section F, Deliverable 47)**.
   3. Support the Government Technical Lead and ISO in uploading assessment results including **STIG/SCAG Self-Assessment Results** (**Section F, Deliverable 48)**, **Security Content Automation Protocol (SCAP) Self-Assessment results** (**Section F, Deliverable 49)**, and **ACAS Scan Results** (**Section F, Deliverable 50)**.
   4. Support the Government Technical Lead and ISO with responding to **Self-Assessment Procedures (Section F, Deliverable 51)/Control Correlation Identifier(s) (CCIs) (Section F, Deliverable 52)** for controls.
   5. Support the Government Technical Lead and ISO with creating **POA&Ms (Section F, Deliverable 53)** and performing remediation and/or mitigations for open findings with POA&M updates.
   6. Support the Government Technical Lead and ISO with reviewing the POA&Ms and validating results within eMASS.
   7. Support the Government Technical Lead and ISO with reviewing the Risk Assessment Tab in eMASS.
   8. Support the Government Technical Lead and ISO with completing the **Assessment Readiness Criteria (ARC) Checklist (Section F, Deliverable 54)**.
   9. Support the Government Technical Lead and ISO with notifying ISSM, via the ticket management system, that all Step 3 tasks are complete.
   10. Support the Government Technical Lead, ISO, ISSO, ISSM, SCAR, Cyber Architect, and ISSE by attending the ARR meetings.

e. RMF Step 4 – Assess
   1. Support the Government Technical Lead, ISO, SCA-R, ISSO, and ISSM in attending Assess Security Control Meetings.
   2. Support the Government Technical Lead and ISO in performing remediation and/or mitigation and updating eMASS based on the findings.
   3. Support the Government Technical Lead and ISO in updating POA&Ms in eMASS.
   4. Support the Government Technical Lead and ISO in updating the Risk Assessment Tab in eMASS to reflect the current security posture.
   5. Support the Government Technical Lead, ISO, and SCAR in submitting the POA&M to the SCAR/Validator(s) for review.

f. RMF Step 5 – Authorize
   1. Support the Government Technical Lead and ISO with finalizing/updating the **Security Authorization Package (Section F, Deliverable 55)** and submitting it to the ISSM and ISSO for review.
   2. Support the Government Technical Lead, ISO, SCA (CISO), Authorizing Official (AO), ISSO, ISSM, and Cyber Architect by attending the Authorization Meeting(s) to brief the AO.

g. RMF Step 6 – Monitor
   1. Support the Government Technical Lead and ISO with monitoring all technical, management, and operational security controls employed within and inherited by systems in accordance with the **Continuous Monitoring Plan (Section F, Deliverable 56)**.
   2. Support the Government Technical Lead and ISO with conducting ongoing assessments in accordance with the SLCM and DCSA policy.
   3. Support the Government Technical Lead and ISO with analyzing and responding appropriately to the output on continuous monitoring activities.
   4. Support the Government Technical Lead and ISO with ensuring the system security documentation is updated and maintained based on the results of continuous monitoring.
   5. Support the Government Technical Lead, ISO, ISSO, ISSM with planning and developing a **Decommissioning (DECOM) Strategy (Section F, Deliverable 57)** and conducting the implementation of that strategy.
   6. Support the Government Technical Lead and ISO to complete decommission activities.

C.5.2.5.1 CYBER REMEDIATION

The contactor shall work collaboratively with a third-party contractor that evaluates devices, systems, and products for security and Supply Chain Risk Management vulnerabilities to engineer and implement possible mitigations to resolve vulnerabilities. The contractor shall actively remediate vulnerabilities within the applicable DoD/DCSA timeframes and in accordance with U.S. Cyber Command (CYBERCOM) IAVM notices, directives, and orders. The contractor shall provide visibility of Operating System (OS) updates and impacts to the enclave. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report).**

The contractor shall implement resolutions and update cyber remediation procedures (i.e., software, hardware, and network), if required; such that processes and solutions will provide confidentiality, integrity, availability, authenticity, access control, survivability, and non-repudiation of information. The contractor shall use **After Action Report (AAR) (Section F, Deliverable 19)** and **Root Cause Analysis (RCA) (Section F, Deliverable 20**) to report this information. Security shall be provided to protect all information and data in accordance with Federal, DoD, Joint Chief of Staff, DISA, Designated Approval Authority (DAA), and Mobility Program Management Office (PMO) security policies. Fully integrated and complaint with Host Based Security System (HBSS) and IA/Intrusion Detection (ID), as well as the ACAS.

C.5.2.5.2 PUBLIC KEY INFRASTRUCTURE (PKI) SUPPORT

The contractor shall integrate, operate, and troubleshoot systems and applications used in the Public Key Infrastructure (PKI) environment. The contractor shall provide technical assistance, including but not limited to, the O&M of the system/infrastructure software and hardware certificates, device certificates, as well as the maintenance of PKI (software and hardware) certificates in support of the infrastructure and approved mobile devices in compliance with DCSA's Key/Certificate Management Plan. The contractor shall recommend and make updates to **DCSA's Key/Certificate Management Plan (Section F, Deliverable 58**). The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

C.5.2.6 SUBTASK 6 – DISASTER RECOVERY (DR) PLAN AND IMPLEMENTATION

DCSA is classified as a Mission Assurance Category (MAC) II, as defined in DoDI 8580.1IA in the Defense Acquisition System and NIST SP 800-59, which addresses mission critical systems. The contractor shall build and maintain a DR plan for an active "hot" recovery site that can be leveraged during normal operations at DCSA (**Section F, Deliverable 59, DR Plan)**. The contractor shall implement the approved DR Plan immediately upon Government or Service Desk notification or through self-analysis that production services have failed. This includes restoration of all DCSA production systems and data. The contractor shall update and maintain the IT system DR Plan and be available to perform testing and validation of its plan and procedures. The DR plan shall be maintained and executed in accordance with DoD policies and mandates and in alignment with DoD RMF, continuous monitoring, and ATO accreditation processes **(**in accordance with **TO Section C.5.2.5)**.

DCSA is currently evaluating an Active/Active datacenter capability from VMWare/CloudPod and Site Recovery Manager (SRM) to provision computers and replicate data in multiple datacenter locations. The contractor shall work with the Original Equipment Manufacturer (OEM) to build a plan and build the Active/Active datacenter configuration, which will enable a "hot" recovery site that will eventually be cloud enabled. The contractor may be required to plan for new "cold" or "warm" site solutions as well as maintain any "cold" or "warm" site solutions currently in operation.

The contractor shall:

a. Conduct training and establish scheduled DR tests, track and report DR test results and lessons learned, and incorporate lessons learned into the **DR Plan (Section F, Deliverable 59)**.

b. Recommend for the Government's approval data (e.g., File System, Database, and Flat Files) replication, backup, and retention requirements.
c. Design, engineer, implement, and maintain storage and backup solutions.
d. Support relocation planning and transition DR infrastructure.
e. Monitor and manage hard drives, tape library, and library physical drives (i.e., failures and replacements).
f. Monitor DR availability, capacity, and performance and provide reports and trend analysis for capacity planning (**Section F, Deliverable 60, DR Availability, Capacity Reports)**.
g. Perform failover tests and provide feedback to the IA Branch.
h. Perform enterprise DR data analysis (search and purge) to reduce capacity.
i. Provision (and de-provision), install, and configure DR solutions in accordance with STIG compliance.
j. Provide ad-hoc reporting as required **(Section F, Deliverable 61, DR Ad-hoc Reports**).
k. Provide engineering capability assessments to ensure DR capabilities are meeting current agency capacity demands and plan, design, and implement capabilities when the capacity demand is no longer being met.

C.5.2.7 SUBTASK 7 – IT OPERATIONS RUN BOOK

The contractor shall maintain and update the **IT Operations Run Book**, as required to stay current with systems and processes (**Section F, Deliverable 62)**. The IT Operations Run Book provides detailed instructions on the IT system and processes.

C.5.3 TASK 3 – ARCHITECTURE AND ENGINEERING (A&E)

A&E currently supports the OCIO strategic objectives of the DCSA IT modernization and DCSA One IT initiatives and provides updates to OCIO and A&E leadership. The contractor shall provide the expertise, best practices, and agility to meet the constant changes and evolution of the enterprise IT environment. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall maintain working partnerships at all levels of the DCSA organization (e.g., strategic, tactical, operational, and with third-party contractors) in order to cohesively design and implement networks, systems, applications, and technology to integrate and improve DCSA's IT enterprise. The contractor shall coordinate with third-party vendors to ensure technology roadmaps are part of the overall Lifecycle Management (LCM) plan. The contractor shall assist with developing and maintaining the **Enterprise Architecture Plans and Technology Roadmaps (Section F, Deliverable 63)** and continually evaluate business cases for new technologies in the enterprise. The contractor shall maintain awareness and transparency performance metrics. The contractor shall leverage the IOD (in accordance with **TO Section C.5.2.3.5**) to improve transparency and situational awareness.

The contractor shall develop project documentation to initiate projects. The contractor shall work cooperatively with third-party vendors and OCIO representatives to support engagements that will improve the operation of OCIO virtual platforms. The establishment of these platforms shall support zero trust measures.

C.5.3.1 SUBTASK 1 – TECHNOLOGY PACKAGES SUPPORT

The contractor shall develop and prepare the technology packages for DCSA's **Technical Review Board Packages** (**Section F, Deliverable 64)**. The contractor may coordinate with the User Experience Division **(**in accordance with **TO Section C.5.2.2)**. The contractor shall prepare the decision brief, design plans, and other supporting documentation required by the RMF in MS PowerPoint (or an automated format) **(**in accordance with **TO Section C.5.2.5)**. The contractor shall prepare to implement the plan(s) upon Government approval. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

C.5.3.2 SUBTASK 2 – NETWORK ENGINEERING

DCSA's network infrastructure consists of non-virtual and virtual systems in multiple DCSA enclaves and data centers, regional field offices, field offices, and the AWS Govcloud environments. DCSA's enclaves include Pre-Production, Production, NIPRNet, SIPRNet, JWICS, and DCSA's multiple cloud instances. DCSA's datacenters supported by this TO are located in RKB Quantico, VA; Ft. Meade, MD; Boyers, PA; Seaside, CA; Farmers Branch, TX; and Phoenix, AZ (anticipated in CY 2022). Onsite network staff are required at DCSA's major field offices (i.e., RKB Quantico, VA; Ft. Meade, MD; Linthicum, MD; and Boyers, PA). Contractor staff shall travel to CONUS field offices, as required, to support network engineering. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall provide network engineering support for all enclaves. The contractor shall conduct planning, design, configuration, troubleshooting, implementation, and security for all DCSA networks. All network services shall be performed in accordance with the latest DCSA and DoD policies and procedures. The contractor shall provide network optimization solutions to A&E management to assist DCSA in moving to a modern virtualized network. The contractor shall recommend changes, enhancements, and improvements to existing network equipment to optimize performance and security. Once any recommendations are approved by the Government, the contractor shall implement the recommendations.

The contractor shall:

a. Develop **Plans, Designs, and Architecture documentation for All Network Enclaves (Section F, Deliverable 65)** in support of this task. Documents include, but are not limited to, network and system specifications, topologies, diagrams, and policies.
b. Perform integration and testing on all equipment, systems, software, hardware, configurations, appliances, and other items in coordination with the appropriate parties.
    1. Ensure network infrastructure is secured and operational before deploying and handing off to operations.
c. Develop and design load balancing (e.g., F5 Big-IP Local Traffic Manager (LTM)) and global and local traffic load balancing engineering and architecture for all enclaves).
d. Assist the Government with coordinating outside agencies, third-party carriers and providers, and vendors to architect engineer and design **Network Blue Prints and Design Documents (Section F, Deliverable 66)**.

e. Design router/switch configurations, firewalls, Internet Protocol (IP) addresses, and related services, such as Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP).
f. Design and engineer all DCSA internet, NIPR, SIPR, and JWICS Regional Internet Access Points (RIAPs).
g. Design, install, and configure new or major changes to site-to-site Virtual Private Networks (VPNs) and gateway servers.
h. Consult with DCSA IT groups to develop and implement a standard architecture for access control points, such as firewalls and Access Control Lists (ACLs).
i. Provide logical **Network Data Flow Diagrams** for each application assessed (**Section F**, **Deliverable 67)**.
j. Conduct data trend analysis on network management activities (i.e., using monitoring tools) and provide reports (**Section F, Deliverable 68, Network Management Trend Analysis Reports)**.
k. Develop engineering capability assessments and capacity planning to ensure the network capability is meeting current agency demands; plan, design, and implement capabilities when the demand is no longer being met; and ensure network provisioned gear is documented.
l. Design, implement, and configure security and firewall solutions in coordination with Cyber Security Defense Operations (provided by a separate contractor/TO support).
m. Develop **Network Configuration Change Control Documentation** (**Section F, Deliverable 69)** when a new configuration changes how a system works.
n. Create configuration documentation that is accurate and complete and coordinate with Configuration Management (CM) to ensure that any new or updated records for configuration items are recorded in the CM system.
o. Develop initial DCSA accreditations and documentation and collaborate to hand-off to Enterprise Operations (in accordance with **TO Section C.5.4**) to ensure accurate artifacts are uploaded to the DoD repository (i.e., eMASS) **(**in accordance with **TO Section C.5.2.5**).

C.5.3.3 SUBTASK 3 – NETWORK SECURITY

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall:

a. Conduct initial **Network Vulnerability Assessment Audits (Section F, Deliverable 70)**.
b. Initially install, configure, and test patches and changes required by Vulnerability Management System issuances (i.e., Information Assurance Vulnerability Alerts (IAVAs), Information Assurance Vulnerability Bulletins (IAVBs), IAVMs, and STIGs) in accordance with the suspense date articulated by the Government authority. All patches, where applicable, shall be tested in pre-production and scheduled with the Government prior to deployment and handoff to the Enterprise Operations team.
c. Review and provide recommendations to improve current processes and procedures.

d. Provide ad-hoc **Network Security Reports** (such as network performance assessments) (**Section F, Deliverable 71)**.

C.5.3.4 SUBTASK 4 – STORAGE ARCHITECTURE AND ENGINEERING (A&E)

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**). The contractor shall engineer storage solutions across multiple platforms (e.g., VMWare Vsan, Dell Unity, and NetApp); however, DCSA's goal is to architect storage using vendor agnostic hardware/software. The contractor shall provide data capacity architecture services, ensuring sufficient data capacity and performance requirements can meet mission demands, including possible surge operations at any given location.

The contractor shall:

a. Design and engineer storage and backup solutions with a preference towards pure flash storage solutions.
b. Develop new storage architectures (including Storage Area Networks (SAN) interconnections) for DCSA enclaves.
c. Perform trend analysis and make recommendations for capacity planning for all enclaves.
d. Provide engineering capability assessments to ensure storage capabilities are meeting current agency capacity demands and plan, design, and implement capabilities when the capacity demand is no longer being met.
e. Scale storage solutions based on the size/ingest of content and the mission.
f. Provide initial storage management services including, but not limited to, design, development, and creation.
g. Provide **Storage Metrics** (**Section F, Deliverable 72)**, such as growth and usage of capabilities, to ensure capability is meeting current agency demands.
h. Provide storage optimization solutions to A&E management and research and recommend new capabilities, as needed.
i. Create and document data capacity management standards baseline for current infrastructure.
j. Aggregate and incorporate all new implementations into baseline standards.
k. Build a comprehensive data capacity management process that is a repeatable building block for future endeavors, to ensure operational demands are meet from a strategic, operational, and tactical level.
l. Deliver and provide recommended configuration changes to enhance and improve infrastructure capacity and performance across the DCSA Enterprise.
m. Provide risk assessment for all data capacity planning actions.
n. Support engineering for Virtualized Multi-Tenant Data Centers (RKB and Boyers) and a Data Center at Ft. Meade with various secure hybrid Cloud Computing solutions, virtualized storage, networks, and desktops in DCSA's environment deployments, including server-accelerating Random-Access Memory (RAM)-based VDI data storage, with server RAM as the primary storage tier and virtualized server acceleration.
o. Engineer SAN including Electromagnetic Compatibility (EMC), with the broad understanding of other SAN leaders including NetApp. Use a broad understanding of

Hyper-Converged solutions and pure flash storage VDI-specific solutions (e.g., Tintri and Nimble Storage).

C.5.3.5 SUBTASK 5 – WEB CONTENT/SHAREPOINT DEVELOPMENT

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**). The contractor shall provide web content support and SharePoint development services to be performed in conjunction with a third-party contractor. For web content, DCSA currently uses Defense Media Activity Platform; however, the contractor may be required to support the implementation of other new technology solutions/platforms within DCSA's current and future environments. The following technologies are required to support DCSA's IT environment for this work: Adobe Creative Suite, Adobe Creative Cloud – Dreamweaver, and other Adobe specialized tools; MS Office Suite; MySQL; Visual Studio; Windows OS; and any other web solution technology approved by DCSA.

For SharePoint, DCSA currently uses the DoD/DISA, Enterprise Portal Services; however, the contractor may be required to support the implementation of other new technology solutions/platforms within DCSA's current and future environments.

The contractor shall provide web content development services including scripting and coding in HyperText Markup Language (HTML), JavaScript, and Cascading Style Sheets (CSS). The contractor shall perform custom configurations on the platforms and deliver customized applications.

The contractor shall provide migration services as requested for existing and future DCSA web content on current and future platforms and environments. The contractor shall provide content and database server administration services. The contractor shall maintain and advise the database team on the health and recommended ways forward with DCSA's web databases to ensure maximum health.

C.5.3.6 SUBTASK 6 – CLOUD COMPUTING

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**). The contractor shall provide A&E support for cloud initiatives approved and directed by DCSA including, but not limited to, AWS Govcloud, MS Azure, and/or VMWare (i.e., Workspace One-related cloud initiatives). The contractor shall be responsible for implementing a cloud services solution under this contract. Cloud computing A&E services are anticipated to be performed in conjunction with a third-party contract and O&M shall be supported under Enterprise Operations **(**in accordance with **TO Section C.5.4.4)**. The contractor shall liaise and coordinate with a third-party vendor and OEM to provide input into re-engineered designs and provide subject matter expertise, when required. The contractor shall implement OEM's best practices (e.g., build and procure the right equipment based on OEM recommendations/best practices). The contractor shall evaluate cloud technologies, determine the best fit for DCSA's environment, build-out, test, and implement the virtual infrastructure (compute and storage) that can support DCSA workloads.

The contractor shall manage and maintain any cloud platforms run by OCIO. The contractor shall interface and integrate OCIO cloud instances and applications with the cloud platforms and applications managed by the PEO/NBIS presently in AWS (and other DoD approved clouds in

the future). The contractor shall perform work to ensure the interface is operable so that data and integrated cloud services are accessible across DCSA's networks.

C.5.4 TASK 4 – ENTERPRISE OPERATIONS

Enterprise Operations maintain DCSA's most critical IT infrastructure and provide updates to OCIO and Enterprise Operations leadership. The contractor shall provide the expertise, best practices, and agility to maintain the constant changes and evolution of the enterprise IT environment to meet the demands of the DCSA mission. The contractor shall maintain working partnerships at all levels of the DCSA organization (i.e., strategic, tactical, and operational) in order to cohesively manage and maintain networks, systems, applications, and technology within the enterprise. The contractor shall work with all parts of DCSA, including other third-party contractors, to assess, update, and improve DCSA's systems. The contractor shall maintain awareness and transparency performance metrics. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall leverage the IOD **(**in accordance with **TO Section C.5.2.3.5)** to improve transparency and situational awareness. The contractor shall update and maintain SOPs for all tasks within Enterprise Operations and facilitate DCSA's requirements for proactively managing and monitoring activities surrounding core business operations. The contractor shall, upon Government approval and in accordance with change advisory board (CAB) policy, implement systems upgrades and maintenance during off-peak hours and weekends, as necessary, to minimize interruption of IT services. The contractor shall develop, update, and maintain the existing SOPs in line with industry best practices, DoD guidelines, and process improvements (**Section F, Deliverable 73, Enterprise Operations SOPs**) **(**in accordance with **TO Section C.5.2.3.8)**. The contractor shall update the DCSA Operations Run Book as necessary **(**in accordance with **TO Section C.5.2.7).**

C.5.4.1 SUBTASK 1 – SERVER OPERATIONS AND ADMINISTRATION

Infrastructure serves as the foundation and building blocks of an integrated IT solution. It is the hardware that supports applications and IT Management Services; the software and services that enable that hardware to function; and the hardware, software, and services that allow for secure communication and interoperability between all business and application service components. The contractor shall provide IT infrastructure services including complete life cycle support for all hardware, software, operations, and administration, including testing, O&M, information assurance, and final disposition of these components. The contractor shall provide administration and service desk functions necessary to support the IT infrastructure. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

DCSA's server infrastructure consists of virtual and non-virtual servers in cloud development environments, pre-production and testing, production, and fail-over enclaves. The contractor shall be responsible for infrastructure asset lifecycle maintenance and ensuring the infrastructure is maintained and secured in all enclaves. The contractor shall provide reliable, high availability services and optimize server infrastructure to achieve high performance and cost-efficiencies for virtual and non-virtual systems. The contractor shall improve scalability, surge, and automation capabilities to support the potential expansion of capabilities and storage throughout the life of

the contract. The contractor shall maintain all configurations in accordance with DoD policies and procedures and consistent with the RMF in accordance with **TO Section C.5.2.5**. The contractor shall support all cloud migration initiatives approved and directed by DCSA.

To support operations and infrastructure, the contractor shall:

a. Provide maintenance to all server infrastructure components (i.e., OS down to the firmware), maintain a secure server configuration, and test and deploy all required patches and updates.
b. Monitor enterprise operations, system configurations, and traffic; provide optimization in health and performance; and provide recommendations for improvements.
c. Provide domain administration services including, but not limited to, system and data access, share management, **Elevated Privilege Accounts Report (Section F, Deliverable 74)**, access/activity log searches, account creation, and user access rights.
d. Provide controls, access, and management enterprise input and output resources (e.g., scanners, printers, files).
e. Add, move, and change printer devices through a print server.
f. Provide capacity management for enterprise computing resources, including proactively recommending and planning upgrades and replacements.
g. Provide encrypted system backups and off-site storage in accordance with DCSA policies and procedures that include incremental and full backups.
h. Provide system and data restoration in accordance with performance requirements established by the RMF.
i. Provide archiving of file data and user information in accordance with DCSA policy and procedures.
j. Ensure the VDI environment is maintained to meet agency demands and performance.
k. Perform physical environment maintenance for shared spaces, in accordance with policies set at each location (e.g., cleanliness and cable management).

C.5.4.2 SUBTASK 2 – STORAGE OPERATIONS AND ADMINISTRATION

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall:

a. Perform O&M for the distributed storage enclaves.
b. Perform Network Attached Storage (NAS) and Fabric Attached Storage (FAS) management.
c. Perform enterprise storage data analysis (search and purge) to reduce capacity.
d. Maintain storage and backup solutions.
e. Maintain all existing storage architectures, including SAN interconnections.
f. Monitor storage availability, capacity, and performance on enclaves and provide reports or real-time analysis as events occur.
g. Monitor and manage physical drives (i.e., failures and replacements).
h. Provision, install, and configure storage solutions in accordance with STIG compliance.

i. Coordinate with third-party vendors and technology providers to troubleshoot and perform operational activities.
j. Coordinate and conduct actions to resolve incidents in coordination with DCSA management, including on storage-related issues.

C.5.4.3 SUBTASK 3 – DATABASE MANAGEMENT

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**). The contractor shall provide database management services for databases residing on DCSA networks. The contractor shall provide database administration support, including modifications to any system or production application database and pre-production database. The contractor shall perform schema changes and conversion of the production database during application upgrades and new version releases.

The contractor shall:

a. Optimize and maintain databases, clusters, and replications for pre-production, productions, and backup; ensure current application upgrades and releases are timely; and provide scripting to support database content and reporting.
b. Provide lifecycle database management services including, but not limited to, provisioning, modifying, and managing data and schema, cloning and backup, troubleshooting, account management, and decommissioning.
c. Monitor, collect, and report **Database Metrics (Section F, Deliverable 75)**, such as growth and usage of capabilities, and coordinate with A&E to analyze.
d. Coordinate with third-party vendors on database issues and resolution. Provide **Database Issues and Resolutions Documentation (Section F, Deliverable 76)**.
e. Develop and maintain database dictionaries for all databases in support of this task (**Section F, Deliverable 77, Database Dictionaries**).
f. Conduct daily database operations checks and status reports.

C.5.4.4 SUBTASK 4 – NETWORK OPERATIONS AND ADMINISTRATION

DCSA network infrastructure consists of non-virtual and virtual systems in multiple DCSA's enclaves, data centers, all regional field offices, field offices, and in the AWS Govcloud environments. DCSA's enclaves include Pre-Production, Production, NIPRNet, SIPRNet, JWICS, and DCSA's multiple cloud instances. DCSA's datacenters supported by this TO are in RKB Quantico, VA; Ft. Meade, MD; Boyers, PA; Seaside, CA; Farmers Branch, TX; and Phoenix, AZ (anticipated in CY 2022). Contractor staff shall travel to CONUS field offices, if required, to support network upgrades, replacements, and maintenance activities. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall support all network cloud migration initiatives and provide ongoing maintenance to cloud initiatives as approved and directed by DCSA, including, but not limited to, AWS Govcloud, MS Azure, and/or VMWare (i.e., Workspace One-related cloud initiatives). The contractor shall maintain, support, and operate all DCSA networks and circuits including DCSA AT&T Multiprotocol Label Switching (MPLS) and DCSA DISA MPLS meshed. The

contractor shall support DCSA in transition from AT&T MPLS to DISA MPLS. The contractor shall support DCSA's data center migration.

The contractor shall be responsible for network infrastructure asset lifecycle maintenance and ensure the network infrastructure is maintained and secured in all enclaves. The contractor shall provide the technical expertise to ensure network infrastructures are reliable, highly available, and optimized to achieve high performance and cost-efficiencies for virtual and non-virtual systems. The contractor shall improve scalability, surge, and automation capabilities to support the potential expansion of network infrastructure capabilities throughout the life of the contract. The contractor shall maintain all configurations in accordance with DoD policies and procedures and consistent with RMF policies in accordance with **TO Section C.5.2.5**.

The contractor shall:

a. Manage and maintain all DCSA network infrastructure and equipment including, routers, switches, firewalls, VPNs, and load balancers on DCSA's enclaves, which include Pre-Production, Production, NIPRNet, SIPRNet, JWICS, and DCSA's cloud instances.
b. Execute regular weekly/monthly patching and security updates for all network systems and devices on DCSA's network infrastructure. All patches, where applicable, shall be tested in pre-production and scheduled with the Government prior to deployment
c. The contractor shall harden network systems/devices according to DOD DISA STIG guidance.
d. Install, configure, and test patches and changes required by the Vulnerability Management System issuances (e.g., IAVA, IAVB, and Technical Advisory (TA) in the context of a DoD IAVM Program) in accordance with the suspense date articulated by DCSA management.
    i. Conduct initial vulnerability assessment audits.
e. Maintain, update, and upgrade all physical and virtual network devices, firmware updates, OS changes, and security releases.
f. Draft, update, and maintain **Network Diagrams, Plans, Designs, and Architecture Documentation** for all enclaves **(Section F, Deliverable 78**) for all network systems and devices.
    i. Update, draft, deliver, and maintain logical network data flow diagrams for each application assessed
g. Create and update SOPs for network operations and administration activities **(Section F, Deliverable 79, Network Operations/Administration SOPs)**.
h. Maintain network documentation and operations under one central location in the IOD **(**in accordance with **TO Section C.5.2.3.5)**.
i. Create and maintain a current, up-to-date **Network Operations/Administrations Runbook (Section F, Deliverable 80)**. The Network Operations Runbook shall be a guidance document for implementing network operations across DCSA. The Runbook shall consist of standards to deploy routers, switches, and network devices to a field office or a data center. The contractor shall process, for hardening, the device in accordance with DoD policy; process to update equipment; process to inventory and control equipment assets; process to provide redundancies and recover/reconstitute a facility in the event of an outage; process to replace equipment; and process to address the ongoing RMF requirements set forth in **TO Section C.5.2.5**.

j. Provide network support and site survey support to new offices and all DCSA field offices and resident offices. The contractor shall maintain circuits and make changes to existing circuits/order new circuits using the DISA StoreFront; and create and maintain a DCSA circuit inventory in accordance with DISA standards (**Section F, Deliverable 81, Network Circuit Inventory**).

k. Conduct all network infrastructure asset LCM and maintenance duties. The contractor shall ensure that the network infrastructure in all enclaves meets DoD standards for compliance and has not exceeded End of Life (EOL)/End of Support (EOS) timelines.

l. Recommend replacement and upgrade plans for all EOL/ EOS network software and hardware. The contractor shall ensure sufficient bench stock of routers, switches, firewall, and equipment to sustain and optimize network operations.

m. Provide JWICS network operations support, as well liaise with A&E network design and planning personnel to perform activities for the JWICS to the field (J2F) project. The contractor shall support accreditations for the deployment of new network/equipment for the new JWICS field offices.

n. Perform day-to-day network operations and administration activities.
    i. Operate and maintain production and pre-production networks in addition to the cloud environments.
    ii. Provide installation, upgrades, configuration, troubleshooting, maintenance, and optimization on Wide Area Network (WAN)/Local Area Network (LAN) routers, switches, firewalls, circuits, and other necessary equipment.
    iii. Manage router/switch configurations, firewalls, IP addresses, and related services (e.g., DNS/DHCP).

o. Provide, ensure, and practice cable management in all data centers, LAN rooms, and telecom closet (i.e., Intermediate Distribution Frame (IDF)). Apply network standard naming conventions and labeling to all network cables and systems. Label each end of all data center patch cable runs and maintain a separate patch cable color code for each classification level and phone systems. Maintain and keep the appearance of data center and telecommunication closets clean and safe and free of hazards.

p. Provide load balancing (F5 Big-IP) and traffic load balancing support for all enclaves including cloud instances. Provide Cisco and Palo Alto firewall product and network support for all enclaves including cloud instances.

q. Identify and resolve network problems in coordination with the SD as required.

r. Serve as a liaison between outside agencies and coordinate with third-party carriers and providers, vendors, and technology providers to troubleshoot and perform operations and network support activities.

s. Maintain all DCSA egress/ingress access points including internet, NIPRNet, SIPRNet, JWICS, and Regional Internet Access Points.

t. Create and maintain an up-to-date mapping of all DCSA site-to-site VPNs (**Section F, Deliverable 82, VPN Mapping)**. The contractor shall support DCSA VPN operations and services to DCSA's users and maintain and operate all DCSA VPNs to ensure connectivity and resolve problems.

u. Create and maintain an up-to-date mapping of all DCSA **Virtual Private Cloud (VPC) Mapping (Section F, Deliverable 83)** instances.

v. Create and maintain an up-to-date **Rack/Elevation Mapping (Section F, Deliverable 84)** diagram at all DCSA locations.

w. Create and document planned changes and facilitate approvals through the change review board. Maintain all CM and change control documentation including, but not limited to, patching and updating existing and new equipment deployments (**Section F, Deliverable 85, Change Control Documentation)**.

x. Coordinate network operations schedules of network activity to field offices, equipment upgrades, and LCM and report on progress of current activities.

y. Provide trend analysis, analyze capacity, and implement approved recommendations to ensure the network capability meets current agency demands (**Section F, Deliverable 86, Network Operations Trend Analysis**).

z. Utilize network monitoring product and bandwidth management solution product to assist in the troubleshooting and network flow analysis.

aa. Operate and maintain OCIO and NISS cloud instances at DCSA **(TO Section C.5.3.6)**.

bb. Provide IT/Communications Security (COMSEC) support to include, but not limited to:

i. Assist the Government with the establishment of COMSEC accounts, conduct briefings, report changed conditions, and facilitate DCSA's secure communications efforts.

ii. Maintain the DCSA's Cryptographic program records. Oversee the maintenance and monitoring of equipment inventory, system configuration, software baselines, service requests, and procurement records in accordance with agency requirements.

iii. Support DCSA's implementation of the COMSEC programs (i.e., COMSEC Material Control System (CMCS) and Central Office of Record) to meet National Cryptographic Management and Audit Policy requirements.

iv. Manage the agency's Key Management Infrastructure (KMI). The contractor shall ensure 100 percent accountability of all COMSEC material and Controlled Cryptographic Item (CCI) devices.

v. The contractor shall analyze and evaluate technical adequacy and compliance.

cc. Programming and local distribution of COMSEC devices including, but not limited to, Secure Telephone Equipment (STE), Sectera vIPer Universal Secure phone, and network encryptor solutions (i.e., Tactical LAN Encryptors (TACLANEs)). The contractor shall order, receive, load, and manage COMSEC keying material using devices such as the KMI, Simple Key Loader (SKL), and other devices as necessary.

dd. Maintain up-to-date records of COMSEC inventory and submit required accounting reports in accordance with policies and procedures **(Section F, Deliverable 87, COMSEC Inventory and Accounting Reports)**. Administer initial briefings and debriefings to individual users and maintain copies of all records (**Section F, Deliverable 88, COMSEC Inventory Briefing Records**).

ee. Complete required National Security Agency (NSA) COMSEC training within the required performance timelines and ensure each COMSEC Element accounts are in compliance with NSA policies.

ff. Provide technical and administrative support to COMSEC equipment holders. Maintain a stock of COMSEC equipment to provide immediate replacement of operational

equipment for use in establishing emergency circuits and to replace equipment in need of repair.

gg. Update and maintain the SOPs for COMSEC activities (**Section F, Deliverable 89, COMSEC SOPs)**.

C.5.4.5 SUBTASK 5 – CUSTOMER SUPPORT (CS)

At DCSA, CS is integral to enterprise operations as the office interfaces with customers for all service requests related to DCSA's IT environment and mission applications. The contractor shall implement a CS program using industry best practices. The contractor shall identify business practices, technologies, and automation in the services it provides that achieve efficiencies in task performance and improve customer experience. The CRM process includes planning, scheduling, and controlling activities involved with service delivery. To that end, the contractor shall develop, deliver, and implement plans to address change management via a communications process (i.e., how can DCSA perform smoother transition migrations of new technology using the example of migrating from Skype to Microsoft Teams). The contractor shall also develop plans and solutions to offer more improved self-service options to gain operational efficiencies. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report)**.

CS requests are communicated through a variety of continually changing channels (currently walk-in, telephone, email, and web inquiries). The contractor's CS representatives shall work in coordination with the Knowledge Center (KC) (in accordance with **TO Section C.5.4.6**), IT SD (in accordance with **TO Section C.5.4.7**), and Desktop Engineering (DE)/Automation (in accordance with **TO Section C.5.4.8**) to provide timely acknowledgement of service requests, problem identification, root cause analysis, escalation, resolution, and closure for all service requests. Contractor CS representatives shall provide guidance, support, and resolve issues in a timely manner. The CS team shall operate a call center for mission applications including, but not limited to; first call resolution for IT service requests, dispatch-ready technicians to assist HQ and DCSA field support staff. The CS team shall be responsible for the coordination, resolution, and closure of all service requests beyond first call resolution (e.g., provide Add/Move/Change for printers and other devices). Resolution of service requests (within the ticket management system) shall be based on the DCSA prioritization level and performance requirements set by policy and identified by the Government. Table 1 describes the priority levels assigned to requests for hardware and software as well as problem resolution time and resolution criteria:

Table 1 - Customer Support Priority Levels and Resolution

Tier Level	Priority	Definition	Resolution Criteria
4	Critical	A problem that affects the entire floor or a department of users.	Ticket opened within five minutes with a technician onsite within 15 mins if issue cannot be resolved telephonically (if technician is available at location). Issue resolved within four business hours.

Tier Level	Priority	Definition	Resolution Criteria
3	High	A problem that affects multiple users within a single floor or department.	Ticket opened within five minutes with a technician onsite within 30 mins if issue cannot be resolved telephonically (if technician is available at location). Issue resolved within eight business hours.
2	Medium	A general service request or problem that affects a single user.	Ticket opened within 30 minutes with a technician onsite within two business hours if issue cannot be resolved telephonically (if technician is available at location). Issue resolved within three business days.
1	Low	A service request that does not require immediate attention or involves long range planning.	Ticket opened within 30 mins with a technician onsite within eight business hours if issue cannot be resolved telephonically (if technician is available at location). Issue resolved within five business days.

The contractor shall implement information sharing and knowledge management capabilities, continuous process improvement, and performance tracking and monitoring capabilities. The contractor shall customize customer preferences relative to interface requirements and information delivery mechanisms. This service facilitates DCSA's requirements for managing and coordinating customer interactions across multiple communication channels and business lines.

The contractor shall initiate service requests and seek assistance from Government agencies via online communication channels. The contractor shall ensure DCSA's customer satisfaction benchmarks and current metrics are tracked and made transparent in the IOD (in accordance with **TO Section C.5.2.3.5**). The contractor shall ensure the execution of the LCMP **(**in accordance with **TO Section C.5.2.4)**. The contractor shall provide weekly, monthly, and ad-hoc reports as required (**Section F, Deliverable 90, CS Ad-hoc Reports)**.

C.5.4.6 SUBTASK 6 – KNOWLEDGE CENTER (KC)

The DCSA KC is the single reference point for customer service support on DCSA's portfolio of mission applications. This portfolio currently includes the NISP NISS, NISP Central Access Information Security System (NCAISS). The portfolio of applications is subject to change over the course of the TO. The contractor KC support shall be responsible for responding to customer service requests, account management, opening/closing service request tickets (using the enterprise ticket management system), first call resolution, and coordination and escalation of issues when necessary (reference requirements in Table 1- CS Priority Levels, Response, and

Resolution). The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall:

a. Provide O&M support of the KC.
b. Provide Tier I user account administration and creation, assist with user registration, and respond to user account requests.
c. Respond, troubleshoot, and resolve technical user account errors and issues.
d. Document, track, and analyze **KC Customer Service Request Documentation (Section F, Deliverable 91)**.
e. Document and track call metrics and service request/resolutions and analyze trends to implement measures that prevent recurring problems and improve customer experience.
f. Recommend and implement technical and/or management capabilities that improve the KC's operational effectiveness.
g. Provide guidance for documentation and knowledge transfer as required.
h. Collect and process data from multiple sources and generate information to support business requirements.
i. Manage the administration of KC records.

C.5.4.7 SUBTASK 7 – INFORMATION TECHNOLOGY SERVICE DESK (ITSD)

The DCSA ITSD is the single reference point for DCSA enterprise IT-related support. The ITSD receives services requests through all accessible communication channels and utilizes an enterprise ticket management system (Remedy/ServiceNow) to track and monitor service requests. DCSA plans to migrate from Remedy to ServiceNow, and it is anticipated that this migration will be complete prior to TOA. The scheduled hours of operation for the SD are 5:00 a.m. to 8:00 p.m. ET (Monday – Friday), excluding Federal Holidays. The SD shall provide support to the CAF on Saturdays from 8:00 a.m. to 2:00 p.m. This coverage does not need to be entirely covered by the primary SD at RKB. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

Contractor personnel providing ITSD support shall be responsible for responding, prioritizing, and coordinating resolution of service requests residing on DCSA networks (i.e., NIPR, SIPR, JWICS, Battlefield Information, Collection, & Exploitation System (BICES), and Insider Threat-Internal). Contractor personnel providing ITSD support shall provide remote support as well as onsite support for customers at the RKB, CDSE regional and local field offices, other remote locations, and Very Important Persons (VIPs) as necessary. Currently, ITSD support provided is decentralized and on-site at the RKB facility in Quantico, VA. Rollover calls are handled at other sites. The contractor shall ensure ITSD support covers DCSA's geographically dispersed locations identified in Section F. Contractor personnel should be prepared to travel within their respective regions, as needed. Onsite (permanent) support is required in accordance with the locations identified in Section F. During the period of performance of the TO, DCSA regional and field offices will be transitioning to a JWICS environment. DCSA follows the Information Technology Infrastructure Library (ITIL) SD framework of incident management, problem management, request fulfilment, and access management.

The contractor shall create, update, and manage tickets utilizing DCSA's enterprise ticket management system (Remedy/ServiceNow). Tickets shall contain real-time and detailed comments, actions taken, details of any issues including symptoms, other pertinent notes that will assist to resolve any issues, specifics on how the ticket was resolved, and/or the current ticket status.

The contractor shall:

a. Provide O&M support of the ITSD.
b. Provide helpdesk support for all enterprise IT service requests or requests escalated through the KC.
c. Provide ITSD support for Tiers I through IV as identified in the priority table (in accordance with Table 1- CS Priority Levels, Response, and Resolution referenced in **TO Section C.5.4.5**).
    i. Make every effort to resolve issues at the time of the service call. This will be the initial method for resolving issues before assigning a priority level.
    ii. Log and assign priorities for all requests not resolved at the time of the call, based on specific definitions.
    iii. Service requests shall be handled according to the priority assigned to them and escalated, as necessary, to uphold the appropriate resolution time commitments.
d. Provide an estimate of the timing for the provision of assistance and/or services.
e. Utilize the ticketing system to provide a status on service requests for users (i.e., via an automated self-accessible portal or through direct follow-up communication).
f. Provide a user self-help capability, such as Tier 0, and continually enhance self-service capabilities to resolve issues for users to reduce service requests.
g. Provide end-user account administration services (add/change/remove) and password resets.
h. Provide desk side support to resolve customer service requests.
i. Coordinate escalation of service requests to regional technicians, field office technicians, and other third-parties, such as hardware and software suppliers, OEMs, third-party contractors, and other DCSA internal technical support, as required.
j. Document and track call metrics, service requests, and resolutions and analyze trends via automated routing, tracking, and management to implement measures that prevent recurring problems and improve customer experience (**Section F, Deliverable 92, ITSD Service Request Metrics/Resolutions)**.
k. Customize trend analyses and reports based on the request from the Government (e.g., may request details on the type of technical issue, location, and tier) (**Section F, Deliverable 93, ITSD Trend Analysis Reports)**.
l. Utilize automated distribution and scheduling activities (e.g., inbound/outbound correspondence management).
m. Draft and post pre-approved situational awareness alerts and information throughout DCSA on IT-related issues impacting the enterprise. Posting methods include emails, web postings, pop-up alerts, and more.
n. Recommend and, upon Government approval, implement technical and/or management capabilities that improve the SD's operational effectiveness.

o. Provide the DCSA TPOC and FEDSIM COR with a weekly status report on all call and service metrics (**Section F, Deliverable 94, ITSD Weekly Status Report)**.
p. Conduct customer satisfaction surveys and provide the survey results **(Section F, Deliverable 95, Customer Satisfaction Survey Results)**.
q. Maintain call-in responsibility in the event of RKB closure.

C.5.4.8 SUBTASK 8 – DESKTOP ENGINEERING (DE)/AUTOMATION

At DCSA, DE/automation supports deployment, maintenance, and troubleshooting of various technologies across all enclaves (i.e., NIPR, SIPR, and JWICS). Currently, the DE/automation team is an extension of the ITSD team and is responsible for timely resolution of service requests, incidents, and issues. The contractor shall manage, track, and update service requests through the enterprise ticket management system. All DE/automation services shall conform to the latest DoD information security policies and timelines. The contractor shall coordinate with various DCSA teams (e.g., Data Center Operations (DCO) and Computer Network Defense (CND) (provided by a third-party contractor support)) to perform work. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall:

a. Provide day-to-day operations for DE/automation tasks.
b. Provide timely service and resolution of service requests and incidents in accordance with the policy.
c. Create and build images; update, maintain, and secure DCSA enterprise endpoints; and develop non-standard workstation images for standalone machines. The DCSA enterprise desktop image shall be updated quarterly and delivered to VDI.
d. Troubleshoot and make recommendations to the Government for remediation of security or functionality issues in the desktop image.
e. Receive escalated Tier II tickets that are escalated to the DE team and resolve desktop incidents and issues, as well as desktop administration (e.g., handle group policy changes and exceptions).
f. Ensure all service requests and issues are tracked and documented within the ticketing system (standards for tickets are referenced in **TO Section C.5.4.5**).
g. Document desktop system configuration, network configuration, (**Section F, Deliverable 96, Desktop/System/Network Configuration Documentation**) and inventory of software to be supported in coordination with **TO Section C.5.4.4** (**Section F, Deliverable 97, Software Inventory**).
h. Perform patches in accordance with DoD authorized timelines.
i. Utilize automation systems (e.g., Tanium, Systems Center Configuration Manager (SCCM)/Windows Server Update Services (WSUS)) to develop, test, and deploy software packages, security updates, and OS for mass desktop software installations.
j. Analyze deployment failures and take corrective actions.
k. Identify problematic trends and patterns and recommend solutions (**Section F, Deliverable 98, DE/Automation Trends and Resolutions Report**).

l. Recommend and upon Government approval; implement technology, knowledge management, and processes that improve the effectiveness of DE/automation.
m. Research new Automation technologies for possible use in the desktop environment.

C.5.4.9 SUBTASK 9 – TECHNICAL CLASSROOM SUPPORT SERVICES

The contractor shall provide onsite technical classroom support services to training centers at various DCSA facilities for faculty, staff, students, and instructors. At present, DCSA supports three training facilities at the Ft. Meade, MD; Slippery Rock, PA; and Ft. Jackson, SC areas, and this support may expand to any area covered under the scope of this TO (e.g., CDSE, NTC), NCCA). Each location shall have a designated contractor personnel assigned, and CONUS travel may also be required. Services shall be performed across unclassified and classified (i.e., NIPR, SIPR, and JWICS) networks. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

Technical classroom support includes training facility/room and end-user IT support, as well as Audio/Visual (A/V) and Video Teleconferencing Capability (VTC) support across all locations. The contractor shall perform the classroom setup, IT equipment and network configuration, desktop support, teleconference, A/V setup, communications, and room tear-down. The contractor shall support A/V across all locations; however, the contractor shall support a more complex A/V systems at NCCA due to the multiple input feeds at that location. The scope of support does not include formal training offerings.

The contractor shall:

a. Image/re-image laptops with the correct version of the approved image in the current Configuration Management Database (CMDB) and in accordance with current cybersecurity policy for student laptop use.
b. Perform classroom setup.
c. Configure and troubleshoot classroom network.
d. Configure A/V and VTC equipment and other systems in the classroom to support of the instructors.
e. Configure and maintain imaging/cloning devices to support classroom and instructors.
f. Configure and maintain network devices to support classroom and instructors.
g. Configure and maintain wireless network to support classroom and instructors.
h. Configure in-classroom equipment, printers, sound, and other systems in support of instructors.
i. Provide computer and application related desktop support (e.g., assist with password resents, connecting to Wireless Fidelity (Wi-Fi) or wired network, troubleshooting applications, and peripheral support).
j. Provide room tear-down duties varying by location (e.g., reset computer image to a standard version, collect computers and equipment, and lock room).
k. Maintain configuration documentation as needed to support the classroom setup and tear down (e.g., special instructions for software installation and configuration, network configuration, Windows Server Update Service (WSUS), MS System Center

Configuration Manager (SCCM), and other classroom-specific IT support requirements) (**Section F, Deliverable 99, Classroom Configuration Documentation**).

l. Provision and maintain tokens to support classrooms, instructors, and students.

m. Setup and remove audio-phone devices used in classroom spaces (e.g., desktop speakerphones).

C.5.4.10 SUBTASK 10 – APPLICATION SUSTAINMENT AND OPERATIONS AND MAINTENANCE (O&M)

The contractor shall provide application sustainment and O&M support for all DCSA's planned and existing portfolio of applications **Section J, Attachment W**. The contractor's sustainment efforts will involve early engagement with the development teams and close coordination throughout the project lifecycle to ensure successful transition into the O&M environment. All application code changes, or software upgrades will undergo formal DCSA Independent Verification and Validation (IV&V) testing by a third-party contractor as referenced in **TO Sections C.5.4.10.1 and C.5.4.10.2.** Testing shall be performed prior to conducting software maintenance that involves code updates, modifications, or changes. Sustainment support of any DCSA system may require personnel to be cleared at the Top Secret (TS)/Sensitive Compartmentalized Information (SCI) level. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall:

a. Ensure seamless transition, reliability, and availability for enterprise IT applications as well as the most cost-efficient strategy for O&M.

b. Work with stakeholders (e.g., Government, third-party contractors, and OEMs) and provide subject matter expertise on behalf DCSA.

c. Review and provide feedback on project plans, designs, scope, requirements, and deliverables to ensure compatibility and integration with the existing and future enterprise.

d. Draft and maintain a **DCSA Technology Roadmap (Section F, Deliverable 100)** that details current technologies and forecasts modernization efforts and planned/new application requirements for increments of three and five years into the future.

e. Monitor application performance, troubleshoot issues, recommend solutions, and implement Government-approved changes.

f. Provide outage/incident management support.

g. Perform application upgrades and maintenance (e.g., adaptive, preventive, corrective, and bug fixes). Ensure software maintenance is performed in accordance with warranty and licensing agreements and timely LCM.

h. Conduct application vulnerability management activities in accordance with **TO Section C.5.2.5.**

i. Perform timely hardware and software patches in accordance with DoD mandates in order to maintain current DoD compliance.

j. Provide ad-hoc reporting, data management, and back-end data support for stakeholders (**Section F, Deliverable 101, Ad-hoc Application Reporting)**.

k. Detect, troubleshoot, and resolve issues or outages that affect the performance of applications.
l. Collaborate and support agency-wide Enterprise Architecture based upon knowledge of existing and planned infrastructure. The contractor shall measure and analyze application performance, recommend application performance baselines, gain DCSA approval of baselines, and perform sustainment activities in a manner that ensures applications perform to agreeable baseline standards.
m. Perform RMF support in accordance with **TO Section C.5.2.5**. Perform sustainment and support to ensure applications are STIG compliant. Develop POA&Ms, when applicable, and submit them to the appropriate DCSA management.
n. Ensure appropriate confidentiality, integrity, and availability, in accordance with RMF and system accreditation requirements, where applications store data. Ensure sufficient capacity management in coordination with the database team.

C.5.4.10.1 PRE/POST TESTING REVIEWS

Prior to submitting application code changes or software upgrades for production usage, the contractor shall perform preliminary internal testing to identify and address test findings. The contractor shall utilize industry best practices and methodologies in testing. Testing results shall be documented in a Test Report that identifies resolved and outstanding contractor test findings (**Section F, Deliverable 102, Test Report)**. The contractor's Test Report shall serve as an input into the formal IV&V testing, which is performed by a third-party contractor. All application code changes, or software upgrades will undergo formal DCSA IV&V testing. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

A Test Readiness Review (TRR) is scheduled prior to IV&V. The TRR serves as a validation point for stakeholder requirements and presents mock-ups in comparison to the delivered changes. It ensures that the system is ready for testing, by having been delivered, installed, and operating with functioning testing accounts. The Test Report is reviewed prior to formal testing.

Post Test Acceptance Review (PTAR) is conducted at the conclusion of testing. DCSA Operational Test and Evaluation (OT&E) test findings are reviewed, and recommendation is provided for production deployment or referred back to the contractor for rework. Unless granted an exception through waiver, findings assigned a Critical or High severity will be returned to the contractor for rework.

The contractor shall ensure attendance at the TRRs and PTARs to provide institutional knowledge about changes throughout the Sustainment organization.

The contractor shall:

a. Perform installation and integration testing (prior to formal IV&V testing).
b. Document all testing procedures including, but not limited to, test plans and scripts, data collection, checklists, schedule, and testing personnel (**Section F, Deliverable 103, Testing Procedures Documentation)**.
c. Document contractor test findings in the **Test Plan Documentation (Section F, Deliverable 104)**, **Test Report (Section F, Deliverable 102)**, and **Test/Use Cases Documentation (Section F, Deliverable 105)**.

d. Coordinate and provision test accounts for OT&E and user acceptance testing.
e. Identify and document defects and bugs in a **Test Report (Section F, Deliverable 102)** (provided at solicitation release)) and develop plans to address issues. Identify critical issues that would prevent the application from being released into the production environment.
f. Perform security compliance testing and address all known and unknown vulnerabilities.

C.5.4.10.2 TESTING AND VERIFICATION

The contractor shall ensure test environments are maintained and replicate production environments. The contractor shall provide consulting and assessments during application testing phases. The contractor shall coordinate sustainment resources in advance of deployment to ensure project documentation and knowledge transfer is conducted. The contractor shall review and approve final project plans, requirements, and deliverables prior to deployment. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall:

a. Proactively configure and maintain test environments.
b. Develop and maintain documentation pertaining to the project phase.
c. Conduct knowledge transfer.
d. Develop an **Application Sustainment Plan (Section F, Deliverable 106)** identifying scope, resources, and costs.
e. Coordinate deployment of applications into the O&M environment.
f. Provide recommendations to improve application integration and performance prior to deployment.
g. Identify critical issues that would prevent the application from being released into the production environment.

C.5.4.10.3 APPLICATION TRANSITION AND DEPLOYMENT

Prior to deployment, the contractor shall review and validate all application transition phase deliverables, test software and/or hardware, review and validate procedures, and complete knowledge transfer between teams. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall support the Production Readiness Review (PRR) as the final enterprise checkpoint or phase gate preceding production deployment. The contractor shall generate and maintain a checklist (**Section F, Deliverable 107, PRR Documentation**) to support the PRR which validates the following:

a. Service Design/Development deliverables were completed and formally submitted to CM; project baseline artifacts, contractor Test Report, and OT&E test results with PTAR decisions.
b. Test Acceptance has been received from OT&E and Government Acceptance Testing (GAT) (if applicable); designated as a "Pass."
c. System accreditation was issued by the Designated Authority (DA).

d. The O&M staff is ready to deploy the product into production for sustainment.

Upon Government approval, the contractor shall lead and coordinate application deployment activities into production environments. The contractor shall coordinate with O&M transition teams and all relevant stakeholders to ensure the deployment is successful.

C.5.4.11 SUBTASK 11 – RELEASE MANAGEMENT

The contractor shall comply with the DCSA enterprise-wide change, configuration, and release management program. The contractor shall establish collaborative, working relationships across the enterprise and support the broader initiatives set forth by DCSA and DoD. The contractor shall work with the Change Configuration and Release Management (CCRM) office and adhere to DCSA's standards, processes, and procedures in accordance with day-to-day operational change, configuration, and release within the DCSA IT environment. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall provide Release Management activities in support of DCSA applications, systems, or infrastructure releases. The contractor shall support the planning and controlling of releases into pre-production (test) and production environments. The contractor shall coordinate with all appropriate stakeholders the content and schedule of the rollout and testing plan (**Section F, Deliverable 108, Release Management Test Plan)** and all other documentation pertinent to the release. The contractor shall ensure accurate information is coordinated with release packages. The contractor shall oversee all releases and deliver **Release Management Reports (Section F, Deliverable 109)**.

C.5.4.12 SUBTASK 12 – MICROSOFT (MS) ACTIVE DIRECTORY ADMINISTRATION

The contractor shall create and deliver data standards to be used across DCSA. The contractor shall perform MS Label (LBL) Active Directory management including user, group, application, and device (e.g., printer) standards. The contractor shall keep DCSA management informed of domain-wide changes, issues, and resolutions. Services shall be performed across unclassified and classified (i.e., NIPR, SIPR, and JWICS) networks. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

For Domain Administration, the contractor shall:

a. Create standards and manage standards.
    1. Create data schemas for DCSA, recommend improvements to schema, and implement modifications.
    2. Create and manage the forest.
    3. Create and remove domains.
    4. Manage trust relationships with other domains.
    5. Assist with DR plans and practice of trust recovery.
    6. Create and manage directory infrastructure, which includes roles, trusts, and replication topology.

7. Create all top-level Organizational Unit (OU) hierarchies with LBL standard sub-OUs, groups, and appropriate security permissions. This includes adding the OU Admins to the Add Computers group, Group Policy Creator Owners group, and OU Admins mail list. It also includes setting appropriate permissions on the created objects and linking of default Group Policy Objects (GPOs).

b. Provide monitoring and reporting associated with the reliability and security of the domain.
   1. Use the domain admin account only for actions that require the privilege level of the account.
   2. Monitor changes to domain root and domain controllers OU to ensure unauthorized changes do not occur.
   3. Perform day-to-day management of the domain controllers including creation, management, and replication.
   4. Monitor connectivity, synchronization, replication, net logon, time services, roles, schema, database partitions, DNS settings, Service (SRV) records, and trust relationships.
   5. Review Domain Controller (DC) event and security logs and take corrective actions.
   6. Monitor and resolve security situations at all levels of the domain to ensure a stable and secure domain.
   7. Secure remote administration of the DCs and member servers.
   8. Work with the DCSA security team to install and manage security reporting tools used to monitor changes to the Active Directory.
   9. Coordinate and configure alarm distribution to OU Admins for OU-related events.
c. Perform DC Management:
   1. Ensure physical security of the domain controllers in Ops Division space and oversee all domain controllers.
   2. Complete backups and restores on domain controllers and the AD environment as a whole.
   3. Plan and implement full DR plan and practice recovery of DCs and core Directory objects.
   4. Manage group policy at root of domain and for DCs OU.
d. Perform policy monitoring and compliance:
   1. Apply and enforce DCSA standard naming conventions for objects in the domain.
   2. Comply with AD policies and standards as agreed by DCSA.
   3. Monitor compliance with AD policies and standards as agreed by DCSA, including change management, communication, and coordination (i.e., distribution).
   4. Arbitrate disputes between OU Admins.
   5. Provide OU Admins with assistance when requested.
   6. Coordinate with DCSA Cyber Security office to ensure the domain is secure.
   7. Comply with DCSA Cyber Security office orders regarding emergency conditions.
   8. Work collectively with the OU administrators.
e. Plan and manage all migrations and upgrades related to the AD or the DCs.

f. Verify all changes to AD work by testing them in a test domain as appropriate, prior to implementation.

For OU Administration, the contractor shall:

a. Ensure overall security and integrity of the managed OU hierarchy.
   1. Use the OU admin account only for actions that require the privilege level of that account.
   2. Monitor changes to OU hierarchy to ensure unauthorized changes do not occur.
   3. Delegate authority to others for appropriate object administration in their OU hierarchy.
b. Perform account management, including creation/deletion/management of objects (e.g., local user accounts, groups, workstations, servers, printers) in their OU hierarchy.
   1. Regularly perform housekeeping duties to keep their OU hierarchy clear of stale, unused, expired, and other no longer needed objects.
   2. Process requests for access control authorized by data owner.
   3. Process requests for group drive mappings via login script.
   4. Create new computer accounts and join to directory services.
c. Designate which administrators have “account operator” access to the Windows user accounts for users in their office.
   1. Account operators will have privileges that let them make changes to a subset of attributes for the accounts in their OU.
   2. This subset of attributes includes Windows-centric information like home directory location, profile location, terminal server settings and other kinds of user data that isn’t replicated from the root of the DCSA domain.
d. Perform GPO creation, troubleshooting, and management.
e. Publish resource objects from their OU hierarchy in the Active Directory as applicable.
f. Manage GPO links within their OU hierarchy.
g. Coordinate with server and/or data owners to set up permissions.
h. Perform Policy Compliance
   1. Comply with DCSA AD policies and standards.
   2. Apply standard naming conventions to objects in their OU hierarchy.
i. Verify new software deployments and GPO policies work by testing them in a test domain as appropriate.
j. Communicate, report, and coordinate with the following:
   1. Work collectively with the domain admins and with other OU administrators.
   2. Provide the following to DCSA management, when suspecting a desktop related problem stems from a change to the Active Directory or DC configuration. For each event provide:
      i. Event description.
      ii. Logon name of affected user(s).
      iii. Total number of affected users.
      iv. Name of affected computer.
      v. Time of event.

vi. Relevant warnings and errors in event logs.
vii. Relevant warnings or errors displayed on screen.
i. When issues affect more than one user provide and AAR and root cause analysis, if deemed necessary by DCSA (in accordance with **TO Section C.5.2.3.2**).
ii. Provide space usage projections.

k. Assist data owners with archiving to alternative storage (e.g., cloud).
l. Disable user accounts for staff (e.g., remove password).

C.5.4.13 SUBTASK 13 – UNIFIED COMMUNICATIONS (UC)

The contractor shall provide UC support. UC is comprised of VTC, A/V, Collaboration Services, Voice Services, and Mobile Solutions. UC endpoints include VTC and mobile phones and resides on unclassified and classified (i.e., NIPR/SIPR/JWICS) networks. Contractor personnel may travel to perform site surveys, coordinate with other offices within Ops (e.g., SD technologists) to research, troubleshoot, and resolve issues. All VTC support personnel must possess an active TS/SCI clearance and will be required to perform work on NIPR, SIPR, and JWICS. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall:

a. Perform data calls and inquiries to discover VTC equipment that may exist in legacy offices (e.g., Defense Security Service (DSS), National Background Investigations Bureau (NBIB) form a plan to integrate existing equipment from legacy into DCSA networks or support EOL activities.
b. Provide O&M support and training for all UC capabilities including, but not limited to, VTC, Voice, A/V, instant messaging, and mobile communications.
c. For all UC capabilities, create and provide both hands-on and virtual training functions to end-users.
i. Instruct personnel on "how to" use conference room equipment, equipment, transfer a call, conference personnel.
ii. Create desktop instructions and guidelines on all UC technologies (**Section F, Deliverable 110, UC Desktop Instructions/Guidelines**).
iii. Provide training that is accessible to customers via InfoLink and SharePoint.
d. Perform site surveys to support new and existing field sites to design/plan/build, provision, and setup, configure, and deploy equipment.
e. Support equipment upgrades at old sites.
f. Provide support for build-outs.
g. Provide VTC and A/V operations, sustainment, and maintenance, troubleshoot issues and resolve problems; and call scheduling.
h. Design and engineer UC solutions.
i. Recommend improvements to the existing service catalog of offerings and implement new capabilities.
j. Issue mobile phones and coordinate with Asset Management for tracking issuances.

k. Provide complete mobile telephone solution, including deployment, invoicing, and end-user support. Setup deployments, accounts with provider, end-user troubleshooting, configuration, incident response, hotspot management, application support, email configuration, and migration to provider services. Provide wireless billing management including, but not limited to, invoice reconciliation, usage and billing analysis, and recommending efficiencies in wireless usage.
l. Provide coordination and resolution with the DoD Mobility Classified and Unclassified Capability (DMCC/UC) in support of mobile device management services.
m. Troubleshoot and resolve DoD Enterprise Email service requests in coordination with DISA. Provide inventory management, specifications, and compliance for all assigned devices in coordination with asset management.
n. Provide Voice over Internet Protocol (VoIP) desk phone support, including deployments, troubleshooting, configuration, problem management, training, and maintenance.
o. Provide EOL support for all equipment.
p. Provide weekly, monthly, and ad-hoc report regarding UC incident reporting (by category and region) and resolution.

C.5.4.14 SUBTASK 14 – DATA CENTER OPERATIONS (DCO)

DCO currently supports HQ DCE, the DR DCW (DRDCW) (anticipated to relocate to Boyers, PA, Ft. Meade, and RKB in late CY 2021), a small server and storage environment in Linthicum, MD, and cloud environments. The contractor shall be responsible for managing DCE networks (comprised of NIPR, SIPR, and JWICS) and DCW (NIPR only) and all associated infrastructure. DCE is also comprised of NATO, Insider Threat internal, and an FBI network for which the contractor shall only be responsible for managing network access connections. The contractor shall manage the SAN and Server environment located in Linthicum, MD, and the infrastructure residing on cloud environments. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

By the time TO performance begins, DCSA will have transitioned approximately 350 HQ users on NIPR and 650 HQ and Field users on SIPR to VDI. The contractor shall support any incomplete transition of VDI users. Additionally, DCSA plans to move from JWICS to a common operating environment provided by NGA/ DIA. The contractor shall support a local environment (on-premises) and migration to a cloud environment.

C.5.4.15 SUBTASK 15 – DATA CAPACITY MANAGEMENT SERVICES

The contractor shall provide data capacity management support services. The contractor shall ensure sufficient data capacity and performance requirements that can meet mission demands including possible surge operations at any given location.

The contractor shall manage data capacity activities including, but not limited to:

a. Maintain data capacity management standards baseline for current infrastructure.
b. Implement an effective data capacity monitoring/trend analysis process that will provide current capacity metrics and highlight performance issues across IT infrastructure, applications (virtualized/physical), user data profiling, and IT components.

c. Recommend changes in capacity, cultivating service performance and delivery of information to users.
d. Continually monitor IT resource usage enabling a proactive identification of capacity and performance issues.
e. Assess incidents/problems related to throughput performance.
f. Monitor trending information and provide future forecast for growth and expansion across DCSA's IT data centers (**Section F, Deliverable 111, Data Capacity Growth Forecasts)**.
g. Deploy a Virtualized Multi-Tenant Data Center and various secure hybrid Cloud Computing solutions, virtualized storage, networks, and desktops in DCSA's environment deployments to include server-accelerating RAM-based VDI data storage, with server RAM as the primary storage tier and virtualized server acceleration.
h. Deploy virtual capabilities, to include the storage, network, server (applications and databases) aspects and the software required to centrally manage this architecture. Software may include VMware, Citrix Systems Application Delivery Controller, Citrix Xen, and MS Hyper-V platforms and extends to desktop management and deployment of the VDI otherwise referred to Thin, Zero, Multi-Level, or Trusted Thin Clients. Thin Clients to include experience in deploying this capability on existing infrastructure (category 5e cable and fiber).
i. Deploy networks, servers, and storage on SIPRNet to include configuration of said equipment to DoD specifications. Enable seamless connections to a Virtual Desktop Environment.
j. Build training plans and train personnel to manage, the complex backend virtual environment to include Cisco's Unified Computing Systems (UCS), EMC VNX storage area network, VMware vCenter, and VMware Horizon View (**Section F, Deliverable 112, Virtual Environment Training Plans**).
k. Deploy and manage SAN(s) to include EMC, with the broad understanding of other SAN leaders to include NetApp. Use a broad understanding of Hyper-Converged solutions (e.g., Nutanix and EVO) and pure flash storage VDI-specific solutions (e.g., Tintri and Nimble Storage).
l. Provision virtual servers to support Unified Computing (i.e., virtual call managers) and SharePoint deployments to include the conversion from Physical-to-Virtual (P-to-V) on a virtualized data center platform.
m. Deploy virtual capabilities in a rural, and disconnected, disadvantaged and intermittent location where bandwidth and access creates unique challenges. This includes large areas and land masses that are disconnected and separated.
n. Provide CS and troubleshooting for Virtual Servers and VDI client hardware and software and coordinating with Government Network Control Centers and HQs.
o. Plan and coordinate virtualization configurations with enterprise technicians and network infrastructure configurations at each location. Plans and coordinates servers chosen for physical to virtual at onsite enterprise locations.
p. Deploy Personal Computer over IP (PCoIP) technologies (e.g., Teradici). The PCoIP compresses, encrypts, and rapidly transports image pixels to PCoIP end-user devices. They in turn decrypt, decompress and display the image on a screen. Includes adding new devices, updating firmware, adding policies.

q. Perform daily VDI Health Checks, which includes the systematic and daily monitoring of the backend infrastructure and desktop performance.
r. Install, configure, and manage VMware vRealize. vRealize provides complete visibility in one place, across applications, storage, and network devices, with an open and extensible platform supported by third-party management packs. vRealize Proactively identifies and solves emerging issues with predictive analytics and smart alerts, and resolves resource contention with intelligent workload placement, enabling optimum performance and availability of applications and infrastructures.
s. Manage, configure, implement software within all listed areas (brands may change or vary, but like technology): SecureView 2.X, VMware, NetApp, Ivanti AppSense, Avamar, Liquidware Labs Stratusphere, UX/Profile Unity, Atlantis Computing ILIO, Teradici PCoIP Management Console, Windows OS, MS Windows Servers, MS Active Directory, SMS, Exchange, MS Office, EMC Legato Networker, Commvault Simpana 7/8/9/10, EMC Control Center, EMC Navisphere, EMC Unisphere, EMC Replication Manager/SE, Time Finder, and Cisco Device and Fabric Manager, Remedy Action Request System, ServiceNow.
t. Perform first line trouble-shooting activities (if required) for installed environments in conjunction with remote and/or local enterprise technicians.

C.5.4.16 SUBTASK 16 – VIRTUAL DESKTOP INFRASTRUCTURE (VDI) MANAGEMENT

The contractor shall provide virtualization management of the desktop/laptop OS including drivers and patches, application, and configuration management. The contractor shall integrate DCSA approved images into the DCSA virtual desktop/laptop environment so that systems can connect directly to the cloud environment. The contractor shall provide support for all end-user (client) applications for desktops/laptops, and applications hosted in the VDI environment. The contractor shall directly interface with, coordinate, and support the network, server services, and security teams on issues that cross these functional areas while maintaining DCSA Enterprise Architecture standards to ensure a consistent and compatible configuration for across the client infrastructure. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall:

a. Provide automated software deployment support.
b. Provide image creation and compatibility.
c. Provide security compliance to include patching, encryption, configuration management, energy management, remote device management, and reporting/visibility.
d. Provide support on any issues that involves end-user hardware or/software in the virtual environment.
e. Provide technical support services across the DCSA enterprise for agency-wide end-user computing platforms for desktops, laptops, and mobile devices; device configuration; technical refresh and customer data migration from one machine to another; and service activities processed in a seamless manner (cradle-to-grave).
f. Maintain service and quality levels with corrective actions as required

g. Coordinate and work with technicians to develop and maintain GPOs to enforce consistency across DCSA's deployed client hardware inventory (in accordance with **TO Section C.5.4.12**).
h. Enable testing of new hardware and software for possible deployment in the environment.
i. Create a Gold Image for E-VDI monthly utilizing the latest Gold Image template. DCSA desires to move to a state where a single Gold image is maintained; however, the current operating environment requires support for multiple images due to new OSs and VDI requirements.
j. Provide effective management of all loaded software for clients.
k. Provide Tier III support on any issues that involves end-user hardware or/software in the virtual environment (in accordance with **TO Section C.5.4.7**).

C.5.4.16.1 ACTIVE DIRECTORY (AD)

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**). The contractor shall maintain the VDI AD structure, infrastructure, group memberships, policies, and service accounts, including but not limited to the following tasks:

a. Design OU structures that allow proper management of VDI workstations separately from hard boxes.
b. Ensure the architecture of Active Directory is adequate for the demands of VDI. Including, but not limited to, domain replication zones, DC placement and communication, and DC load.
c. Manage AD groups to provide access to the VDI environment.
d. Manage AD Groups to provide administrators required access.
e. Design, create, and manage group policies for users and VDI machines. The current operating environment requires the use of Loop Back Processing for some user accounts, which behave differently than on other workstations within the DCSA environment. DCSA Group Policies enforce security compliance to both user accounts and VDI Computer Accounts.
f. Ensure critical service accounts have required VDI privileges. Ensure passwords meet requirements for security compliance.

C.5.4.16.2 HARDWARE PLATFORM

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**). The contractor shall maintain the VDI hardware platform including, but not limited to, hardware provisioning, procurement, deployments, lifecycle management, and storage provisioning.

The contractor shall perform the following activities including but not limited to:

a. Evaluate server hardware current and future requirements. Design server platforms to meet current and projected load capacity.

b. Unbox, rack-mount, and configure all hardware per best practices. Install hardware OS and required software. Implement in environment following established change management procedures.
c. Maintain and ensure that hardware firmware and drivers are up to date ensuring they meet all security and LCM requirements. Properly decommission old hardware when lifecycle is complete.
d. Conduct storage provisioning. Evaluate Storage capacity and throughput requirements as it relates to VDI. Estimate VDI storage throughput requirements using industry standard tools. Provide leadership with reports regarding storage throughput needs.

C.5.4.16.3 SECURITY

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**). The contractor shall maintain VDI security including, but not limited to, the following:

a. Perform platform patching. Apply MS and third-party patches to VDI gold images. Ensure all security scan findings are resolved in the required time frame. Ensure all VDI appliances meet minimum version levels. Ensure all VDI servers are patched and meet minimum version levels.
b. Perform critical patching. Resolve all IAVM requirements within the mandatory time (zero-day, Short Notice).
c. Perform and maintain STIG compliance. Ensure all VDI gold images meet STIG compliance requirements (in accordance with **TO Section C.5.2.5**).

C.5.4.16.4 PLATFORM DESIGN

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**). The contractor shall design VDI platforms including, but not limited to, the following:

a. Utilize extensive knowledge of Host Based Security System (HBSS) solution management. Ensure HBSS is installed to meet VDI specific requirements.
b. Create Gold Image. Develop, test, and deploy Windows gold image that meets the changing needs of the users. Ensure necessary software/drivers is correctly installed and regularly updated.
c. Manage VDI software. Develop optimum strategy for managing software requirements. Evaluate virtual applications versus locally installed.

C.5.4.16.5 SYSTEM MONITORING

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**). The contractor shall perform VDI system monitoring including, but not limited to, the following:

a. Monitor system performance. Routinely monitor all performance metrics in the VDI environment. Ensure Host Computer (CPU), memory, and Network load is within acceptable levels.

b. Provide performance reporting **(Section F, Deliverable 113, VDI Performance Reporting)**. Routinely provide leadership with system performance reports to ensure continued high availability of the system.
c. Resolve performance issues by working with non-VDI teams to resolve any performance degradation in a timely manner.
d. Build and Maintain VDI Gold Image(s).

C.5.4.16.6 NETWORKING

The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**). The contractor shall perform VDI networking including, but not limited to, the following:

a. Apply networking foundational knowledge by understanding the current and future network layout(s).
b. Validate network operability by working with the Networking team to ensure network hardware meets current and future VDI requirements.
c. Manage Virtual Switches. Design and manage VMWare virtual basic and distributed switches. Establish Virtual Local Area Networks (VLANs), if necessary, within the Virtual Switch network.

C.5.5 TASK 5 – PROGRAM EXECUTIVE OFFICE (PEO) SUPPORT

The contractor shall provide recommendations to the Program Executive Office (PEO) and Directorates across the DCSA to drive transformative change in IT resource planning and execution using the Acquisition and Budget Management (ABM) Tool and the service ticketing (ServiceNow) platform. The contractor shall utilize organizational change management best practices to onboard and support users of the ABM Tool across DCSA, setting the strategic foundation for DCSA-wide ServiceNow adoption.

The contractor shall

a. Utilize ABM tool user story backlog to agilely develop the tool. Gather feedback from across the agency to continuously implement enhancements and improve user experience and overall impact of the ABM Tool **(Section F, Deliverable 114, ABM Tool)**.
b. Maintain and enhance various business process workflows **(Section F, Deliverable 115, Process Workflows)** in support of the ABM Tool across the agency.
c. Utilize the ABM tool as a central source of historical information for agency data.
d. Investigate analytics best practices to create and deliver the best available Dashboards within ServiceNow that convey digestible and interactive graphics for the PEO that will lead to more informed decision-making capabilities.
e. Deliver capabilities such as automated workflows, timely and comprehensive reporting capabilities, and access to reliable historical and future year requirements to enable leadership to better manage and forecast resource needs across DCSA **(Section F, Deliverable 116, ABM Tool Enhancements)**.
f. Find integration opportunities between the ABM Tool and standardized Investment Reporting (IR) processes (e.g., Select & Native Programming Data Input System (Snap

IT), Information Technology Process Action Team (IT PAT)) to drive efficiencies across the DoD enterprise.

C.5.6 TASK 6 – NATIONAL INDUSTRIAL SECURITY PROGRAMS (NISP) NATIONAL INDUSTRIAL SECURITY SYSTEMS (NISS) SERVICES

As one of four Government security agencies directed to implement the NISP per Executive Order 12829, DCSA provides Industrial Security Services and training to the DoD and 33 other Federal agencies. NISS provides seamless integration of other DCSA systems and applications, such as Defense Information Security System (DISS) and planned integrations with National Contract Classification Security System NCCS and eMASS. NISS provides DCSA with comprehensive enhanced capability to manage its entire mission portfolio. NISS improves information sharing and collaboration, by providing timely and accurate data to field representatives for decision-making. The system provides agency-wide metrics to improve agency performance in providing security oversight and the protection of national security.

C.5.6.1 SUBTASK 1 –NISS PROGRAM MANAGEMENT (PM)

The contractor shall provide program and project management functions for NISS to include development of new NISS system capabilities, sustainment of the current system, and to provide training resources for end users **(**in accordance with **TO Sections C.5.1, C.5.2 and C.5.6.8)**. The contractor shall manage NISS resources, license renewals, and the overall schedule of the NISS program. The contractor shall interface between the core Government NISS team and the greater Government DCSA One IT team to ensure timely collaboration and coordination of efforts.

The contractor shall establish continuous training for onboarding team members via in-person, webinar, or computer-based training. The contractor shall allocate a shared location, such as the TO Portal **(TO Section C.5.1.10)** to store User Job Aids, Templates, Meeting Minutes, Meeting Agendas, and other Training Material that is accessible by all team members.

C.5.6.2 SUBTASK 2 –NISS OPERATIONS AND MAINTENANCE (O&M)

The contractor shall perform application development and knowledge transfer for all new NISS application capabilities. The contractor shall provide application sustainment support for NISS application(s) in both the NIPR and SIPR environments. Sustainment involves early engagement with the development teams and close coordination throughout the project lifecycle to ensure successful transition into the O&M environment. The contractor shall work with stakeholders (e.g., Government, third-party contractors) and provide subject matter expertise on behalf of the infrastructure and sustainment team. The contractor shall review and provide feedback on project plans, designs, and deliverables to ensure compatibility and the ability to integrate with the existing and future state.

The contractor shall provide ITSD support (Tier 1 and Tier II) for NISS, in accordance with **TO Section C.5.4.7**. The contractor shall provide the necessary infrastructure support and regular maintenance (adaptive, preventive, and corrective) for NISS applications. The contractor shall provide support to the Technology Roadmap which forecasts NISS application requirements at least three years into the future.

The contractor shall provide the following NISS application(s) services, including but not limited to:

a. Access to the product support team.
b. Respond to telephonic, instant messaging, and email support requests based on a prioritization system (in accordance with **TO Section C.5.4.5**).
c. Patching software in response to any discovered / disclosed security vulnerabilities.
d. Fixing software bugs in response to issues raised by users through the appropriate support processes.
e. Working with OEMs to upgrade and customize existing and new Commercial products including new features implemented in response to feedback from across other Government and commercial customers.
f. Sustaining the NISS development environment deployed cloud instance and work with Enterprise Operations to assist with future migrations to cloud environments.
g. Updating system documentation to reflect changes **(**in accordance with **TO Section C.5.2.5)**.
h. Coding delivery within line code comments.

C.5.6.3 SUBTASK 3 –NISS APPLICATION DEVELOPMENT

The contractor shall perform an assessment of the NISS application(s) platform and provide courses of actions for no less than three options including reporting and metrics capabilities; and provide it to the Government (**Section F, Deliverable 117, NISS Courses of Action)**. The contractor shall procure, configure and deploy the reporting and metrics capability selected by the Government.

Upon Government approval of the technical design documentation, the contractor shall perform Agile development of NISS applications. The contractor shall use industry best practices and methodologies when performing development.

The contractor shall:

a. Deliver an IMS (in accordance with **TO Section C.5.2.3.6**) detailing planned versus actual activities (project scope, schedule, costs, and product quality) (**Section F, Deliverable 118, NISS IMS**).
b. Provide risk management with establishment and maintenance of a Risk Register **(**in accordance with **TO Section C.5.2.5) (Section F, Deliverable 119, NISS Risk Register**) including identified risks, qualitative analysis, triggers, and responses.
c. Escalate issues that arise during development to the Government with an **NISS Issue Impact Analysis Report (Section F, Deliverable 120)**.
d. Develop and maintain a **NISS RBS (Section F, Deliverable 121)** that provides full visibility on resource allocation and schedules.
e. Provide System Accreditation support and documentation **(**in accordance with **TO Section C.5.2.5)** (**Section F, Deliverable 122, NISS RMF Documentation**).
f. Provide documentation on development activities to address knowledge transfer with the O&M team.

In addition, the contractor shall provide the following **NISS Lifecycle Development Documentation (Section F, Deliverable 123)**:

a. Software Code/Software Code Integration between systems.

b. Release Summary Report.
c. System Architecture/Design Documentation with process flow diagrams.
d. Technical Requirements Documentation.
e. Requirements Traceability Matrix.
f. Network Typology.
g. Installation/User Guide.
h. RMF Compliance Documentation.
i. Deployment Plan.
j. Data Dictionary with Meta-data Mapping (Schema).

C.5.6.4 SUBTASK 4 –NISS TRANSITION AND DEPLOYMENT

The contractor shall execute no less than four major deployments per option period with minor releases as needed to address bug fixes and critical capabilities.

The contractor shall ensure that prior to deployment, all transition phase deliverables are reviewed and validated, software and/or hardware are tested, procedures are reviewed and validated, and knowledge transfer is complete between teams. The contractor shall support the PRR as the final enterprise checkpoint or phase gate preceding production deployment. A **NISS PRR Checklist (Section F, Deliverable 124)** shall accompany the PRR as validation of the following:

a. Service Design/Development deliverables were completed and formally submitted to CM; project baseline artifacts, contractor Test Report, and OT&E test results with PTAR decisions.
b. Test Acceptance has been received from OT&E and GAT (if applicable); designated as a "Pass."
c. System accreditation for all platforms was issued by the AO.
d. The O&M staff is ready to deploy the product into production for sustainment.

Upon Government approval, the contractor shall coordinate application deployment activities into production environments. The contractor shall coordinate with O&M transition teams and all relevant stakeholders to ensure the deployment is successful (i.e., Change Advisory Board (CAB) approval is received, package is deployed, in use, timely, without bugs).

C.5.6.5 SUBTASK 5 –NISS DATA INTERFACE

The contractor shall develop data interfaces for no less than two existing systems, where NISS data will be transferred to the system as well as data being transferred from that system to NISS.

The contractor shall:

a. Label data.
b. Support current DCSA efforts of data normalization through support of collaboration of Intelligence Community (IC) and Federal communities in adherence with the current DCSA data catalog.
c. Follow the current enterprise data labeling strategy and implementation plan, coordinate with the development team and maintain **NISS Data Dictionaries (Section F, Deliverable 125)** for each data set, including a data label catalog, coordinate and manage

metadata/tagging of resources for enterprise discovery and sharing and provide updates to the DCSA data management portal.

d. Support gathering requirements through the development of **NISS Operational Requirements documents (Section F, Deliverable 126)** and **NISS Operational Use Cases (Section F, Deliverable 127)**.
e. Request prioritization of data set through collaboration with the DCSA cloud services and data team, collect and track requirements tied to specific data sets for reference.
f. Review submitted Data Request Form(s) (DRF).
g. Determine capacity requirements for each data set.
h. Work with NBIS operations regarding ingest and data methodology and sustainment.
i. Identify the transport for data delivery, identify capabilities required to extract data and direct flow.
j. Identify data destination and staging location(s).
k. Adhere to security policy for access control and authorization decisions.

C.5.6.6 SUBTASK 6 –NISS CLOUD MANAGED SERVICES

The contractor shall use the Government provided cloud management resources for security assessments, update/patch requirements, and other maintenance activities deemed necessary.

The overall NISS Program is moving to a cloud solution to align with DCSA's overall Cloud Strategy. The contractor shall provide management of IT-related services using cloud service providers appropriate to enhance NISS-NIPRnet (NISS-N) and NISS-SIPRnet (NISS-S) security risk management and security professional development services.

Currently, NISS-N is located on premise and utilizes a shared AWS environment for development. The contractor is expected to provide full IT transformation services to cloud platforms for NISS-N, and cloud development for NISS-S. The contractor shall coordinate and collaborate with the DCSA Cloud Services team as it pertains to the management of all cloud services, for both NISS instances by providing responsive, adaptive, and timely solutions in alignment with DoD Cloud requirements. The contractor shall collaborate with the DCSA Cloud Services team to support both classified and unclassified system cloud design, development, research, and sustainment activities.

The contractor shall provide cloud managed services support including, but not limited to, the following:

a. Infrastructure Management: collaborating with the DCSA Cloud Services team to establish a repeatable process to provision cloud environments and confirm that all systems are proactively managed and service levels are maintained.
b. Cyber Security: collaborating with the DCSA Cloud Services team to ensure NISS-N and NISS-S security configurations, processes, and policies within DCSA eMASS are compliant with RMF policies.
c. Service Management: collaborating with the DCSA Cloud Services team to conduct cloud vulnerability scanning and end point protection services in alignment with DoD Cloud Compliancy.
d. Automation and Development and Operations (DevOps)/Development, Security and Operations (DevSecOps): collaborating with the DCSA Cloud Services team to utilize

innovative and cloud service tools to automate LCM, continuous integration, and deployment to quickly meet changing mission needs.

e. Optimization and Transparency: collaborating with the DCSA Cloud Services team to maintain a holistic view into the cloud landscape and document report on empirical data on usage and consumption designed to optimize solution footprints (**Section F, Deliverable 128, Usage and Consumption Data)**.
f. Maintenance and Sustainment of Environments: collaborating with the DCSA Cloud Services team to develop and maintain a development, test, pre-production, and production environment and develop a seamless failover plan to ensure users see no impact for downtown and maintenance times.

C.5.6.7 SUBTASK 7 –NISS SECURITY

As part of the overall NISS, the contractor shall continuously provide industry best practices and experiences in order to meet appropriate DoD cybersecurity (on premise or cloud environment) and RMF compliance standards. The contractor must maintain access into the eMASS system utilizing the program ISO/PM roles and workflows in the support of the creation, modification and sustainment of cybersecurity accreditation packages and artifacts. The contractor shall perform regular third-party penetration testing and vulnerability scanning to verify hosting security and implement targeted OS patches and upgrades. The contractor shall perform cybersecurity risk assessments, continuous monitoring, and vulnerability scanning mitigation to verify hosting security and implement targeted OS IAVA's, patches and system firmware/software upgrades.

The contractor shall provide cybersecurity services including, but not limited to, the following:

a. Risk Assessments: regularly conducting actions identifying and analyzing potential cybersecurity related events that may negatively impact individuals, assets, and the operating environment and execute steps to provide mitigation strategies to the government.
b. System Access Controls: using access controls that manage who can make system changes to segregate roles. These controls shall be fully customizable and offered at a very granular level, allowing administrators to set very specific permissions according to specific users or user groups.
c. Continuous Monitoring: ensuring that the information environment is being continuously monitored for cybersecurity-relevant events and configuration changes that may negatively impact cybersecurity posture. This shall be done by addressing cybersecurity considerations when changes are made to either the security controls baseline or to the baseline of the operational computing environment.
d. Cybersecurity Operations Planning: supporting the creation and sustainment of operational planning documents including, but not limited to, the system incident response plan, **NISS Operational Planning Documents** (**Section F, Deliverable 129)**, **NISS Contingency Plan (Section F, Deliverable 130)**, **NISS DR Plan (Section F, Deliverable 131)**, and **NISS CM plan (Section F, Deliverable 132)**.
e. Risk/Vulnerability Mitigation: supporting the implementation of proposed solutions recommended by way of a vulnerability assessment (e.g., Blue Team activities) and

penetration testing (e.g., Red Team activities) by ascertaining the limitations and capabilities of the fix.

f. POA&Ms: supporting the Government development of a system POA&M that addresses the implementation of cybersecurity requirements throughout the lifecycle of the system.
g. User level Access Controls: segregating roles using access controls that manage who can make system changes. These controls shall be fully customizable and offered at a very granular level, allowing administrators to set very specific permissions according to specific users or user groups. Access Controls. Shall segregate roles using access controls that manage who can make system changes. These controls shall be fully customizable and offered at a very granular level, allowing administrators to set very specific permissions according to specific users or user groups.
h. Change Controls: providing a layered cloud architecture designed infrastructure that reduces the external attack surface and consolidates traffic and connections through various chokepoints to allow for enhanced monitoring and detection. Continuously evaluate and improve the architecture to mitigate risk from both internal and external threats. Enforce deny by default policies and can only be updated through the contractor's change management process.
i. System Logs and Monitoring: providing a logging application that records the date, IP address, user, and outcome (success or failure) of any action that modifies application permissions (e.g., user add, user remove, add to group) or any action that changes the state of the hosting environment (e.g., uploading a file, executing commands on the host). The application shall create a trail of log entries that can be used to support effective responses and hold parties responsible in the case of an incident. Provide automated alerts of high-priority events and facilitate speedy communication, response, and remediation.
j. DevSecOps: providing security practices for every stage of application development. The contractor shall provide a security team that focuses on security policies compliance (i.e., STIG), oversees continuous deployment, and performs advanced manual penetration testing.
k. Maintaining the DoD RMF accreditation for an ATO on DoD NIPRNet and SIPRNet. Includes all data items in accordance with **TO Section C.5.2.5**.

C.5.6.8 SUBTASK 8 –NISS TRAINING

The contractor shall work with Government teams to develop and maintain **NISS User Job Aids (Section F, Deliverable 133),** and **NISS Templates (Section F, Deliverable 134).** As new applications are developed the contractor shall provide User Job Aids or Templates to guide users in how to utilize the new applications. The contractor shall update User Job Aids and Templates on a quarterly basis, or as needed by project requirements. Templates shall include SOPs **(**in accordance with **TO Section C.5.2.3.8)**, Meeting Minutes and Agendas, System and RMF **(**in accordance with **TO Section C.5.2.5)** cybersecurity documentations. Source files for all training materials, including templates, presentation materials and meeting minutes shall be provided to the government and uploaded to the TO Portal (in accordance with **TO Section C.5.1.10)**.

The contractor shall maintain existing **NISS Computer Based Training (CBT) (Section F, Deliverable 135)** for all NISS functionalities and work with the Government to develop new

CBTs for improved functionality as the NISS systems are modernized. The contractor shall review CBT content no less than annually and make any recommendations for improvements.

It is anticipated that during the first year of performance a total of six CBTs will be developed. Three of these training will have a NISS system focus as follows:

a. System level training for industry users.
b. System level training for Government users.
c. System level training for internal users.

Additionally, it is anticipated that no less than three minor CBTs related to specific NISS features will be required. The purpose of the minor CBTs is to assist users with improved features of the NISS system.

C.5.7 TASK 7 – TOOLS/ASSET MANAGEMENT SUPPORT

The contractor shall develop and implement an enterprise-wide IT Asset Management program, inclusive of all IT assets. The contractor shall report the progress of all technical activities performed under this task/sub-task in the Activity Report **(Section F, Deliverable 144, Activity Report**).

The contractor shall coordinate software and hardware maintenance, renewals, and warranties (including repairs) with third-party vendors. The contractor shall assist DCSA personnel with asset inventory support leveraging access to the Defense Property Accountability System (DPAS).

The contractor shall procure IT assets including hardware and software in accordance with the procedures outlined in **Section H.10**. The contractor shall provide records of all agreements and purchases (i.e., MOA's/MOU's) in file records.

C.5.7.1 SUBTASK 1 – LOGISTICS MANAGEMENT

The contractor's asset management program shall track, manage, and coordinate the purchase of new equipment (hardware and software), replacements, and upgrades. Asset management includes the cataloging, identification, tracking, transfer, allocation, license maintenance, and warranty maintenance of IT assets. The contractor shall provide asset inventory and asset tracking documentation (**Section F, Deliverable 136, Asset Inventory and Tracking Documentation**) that tracks information regarding expiration, renewal, reporting, forecasting, and delivery of managed devices, licenses, or warranties under the DCSA One IT Program. The contractor shall work with respective parties and vendors to ensure that all equipment (hardware and software) is appropriately logged into the asset inventory in accordance with DCSA policies and regulations.

C.5.7.1.1 SUPPLY CHAIN RISK MANAGEMENT (SCRM)

This TO is subject to the Federal SCRM policies and regulations including the Defense Federal Acquisition Regulation Supplement (DFARS) 252.239-7017, Notice of Supply Chain Risk; DFARS 252.239-7018, Supply Chain Risk; DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks; Section 806 of the FY 2011 National Defense Authorization Act (NDAA) Requirements for Information Relating to Supply Chain Risk; and internal DCSA SCRM processes and procedures.

The contractor shall submit a **SCRM Plan (Section F, Deliverable 137**), that describes how the contractor shall reduce and mitigate supply chain risk using the security controls outlined below (further described in Committee on National Security Systems Instruction (CNSSI) 1253, Appendix D and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53), as applicable to the contract.

The contractor shall execute the SCRM Plan and provide updates in the event of changes that affects supply chain risk. At a minimum, the following events substantiate the need for an update: changes in company ownership, changes in senior company leadership, supplier changes, subcontractor changes, and supply chain compromises.

If, during the performance of the TO, the contractor experiences a change that creates a supply chain risk that cannot be mitigated, the FEDSIM CO and DCSA must determine whether a continuation of the TO may pose an undue risk to the common defense and security through the possible compromise of that information or material. If DCSA determines that such a threat or potential threat exists, the FEDSIM CO shall consider the alternatives of negotiating an acceptable method for isolating the supply chain risk that influences the contractor, or execute DFARS 239.73, Requirements for Information Relating to Supply Chain Risk.

Control Number		HW	SW	Service
SA-12	Supply Chain Protection	X	X	X
SA-12(1)	Supply Chain Protection / Acquisition Strategies / Tools / Methods	X	X	X*
SA-12(2)	Supply Chain Protection / Supplier Reviews	X	X	X*
SA-12(5)	Supply Chain Protection / Limitation of Harm	X	X	X*
SA-12 (7)	Supply Chain Protection Assessments Prior to Selection / Acceptance/ Update	X	X	X*
SA-12 (8)	Supply Chain Protection / Use of All-Source Intelligence	X	X	X*
SA-12 (9)	Supply Chain Protection / Operations Security (OPSEC)	X	X	X
SA-12 (10)	Supply Chain Protection / Validate as Genuine and Not Altered	X	X	X*
SA-12 (11)	Supply Chain Protection / Penetration Testing / Analysis of Elements, Processes, and Actors	X	X	X
SA-12 (12)	Supply Chain Protection / Inter-Organizational System Components	X	X	X
SA-12 (13)	Supply Chain Protection / Critical Information System Components	X	X	X*
SA-12 (14)	Supply Chain Protection / Identity and Traceability	X	X	X*
SA-12 (15)	Supply Chain Protection / Process to Address Weaknesses or Deficiencies	X	X	X
IR-4 (10)	Incident Handling / Supply Chain Coordination	X	X	X*
IR-6 (3)	Supply Chain Protection / Incident Reporting / Coordination with Supply Chain	X	X	X*
SA-11	Developer Security Testing and Evaluation	X	X	X*
SA-14	Criticality Analysis	X	X	X*
SA-15	Development Process, Standards, and Tools	X	X	X*

Control Number		HW	SW	Service
SI-7	Software, Firmware, and Information Integrity	X	X	X*
CM-4	Security Impact	X	X	X*
PM-16	Threat Awareness Program	X	X	X

*Not required if there will be no procurement of hardware, firmware, or software systems.

C.5.7.2 SUBTASK 2 – LICENSE/WARRANTY ACCOUNTABILITY

The contractor shall track and manage all third-party hardware maintenance and software licensing support by maintaining a 100 percent accountability of all assets. The contractor shall manage and track all system and device/application licenses, including expiration, for DCSA on all networks, and compute infrastructure and production applications. The contractor shall track all endpoint devices and assets for inventory management. The contractor shall maintain all non-user-based IT equipment inventory, including network printers and VTC components in conference rooms.

The contractor shall provide a detailed list of required licenses (sortable by license type and specific device) to the Government and deliver licenses to DCSA for installation on devices and systems prior to license expiration (**Section F, Deliverable 138, License Requirements/Renewal/Data Repository Documentation**). The contractor shall monitor and maintain the equipment (hardware and software) license data repository that records and tracks all information pertinent to the lifecycle maintenance of the product (including vendor name, software name and version, number of authorized users and/or devices covered, licensing fees, commencement, and expiration date, etc.). The contractor shall maintain an up-to-date equipment inventory list and system data that is to be delivered to the Government upon request (**Section F, Deliverable 139, Equipment Inventory Lists**).

The contractor shall provide early notification and coordination with the FEDSIM COR, the DCSA TPOC, and appropriate resource advisor of upcoming expirations of maintenance, warranty, or license agreements within 30, 60, 90, 120, 150, and 180 days. The contractor shall ensure equipment installed on DCSA networks is licensed, and any software without an available license is provided with written permission from the DCSA TPOC. The contractor shall track and maintain a readily available inventory of all equipment issued to DCSA personnel.

C.5.7.2.1 PROPERTY ACCOUNTABILITY

The contractor shall submit an **Electronic Products List (Section F, Deliverable 140**) in addition to complying with all requirements of DFARS 252.211-7003. See Defense Acquisition Regulatory System (DARS) 252.211-9000, Requirement to Submit an Electronic Product List for additional information.

C.5.7.3 SUBTASK 3 – DEMAND AND FORECAST MANAGEMENT

The contractor shall support common practices for ordering assets, tracking orders and assets, and (for hardware/equipment) tagging (including barcoding) the assets. The contractor shall assist the Government in capacity planning, providing analysis of current systems equipment and/or software licenses are optimal to support additional influxes of capacity. The contractor

shall provide accurate and timely responses to ad-hoc data calls for information related to forecasts and projected costs.

C.5.7.4 SUBTASK 4 – SHIPPING AND RECEIVING

The contractor shall ship and receive equipment at the Government's request (e.g., using corrugate, packing material, FedEx shipping forms, etc.). The contractor must have certified personnel to send, receive, and handle cryptographic COMSEC equipment. The contractor shall send the COMSEC equipment in accordance with NSA policy and according to the level of classification of that equipment.

C.5.7.5 SUBTASK 5 – MATERIAL INSPECTION/RECEIVING

The DoD requires contractors who supply goods or services under a contract that contains DFARS clause 252.246-7000 to submit a material inspection and receiving report, a DoD Form 250 (DD Form 250). This form is the receiving document used to record the delivery of goods or services including pertinent information about the TO. In order to comply with the TO the vendor must provide a completed DD Form 250.

C.5.7.6 SUBTASK 6 – END-OF-LIFE (EOL)

The contractor shall process EOL, defective, and/or damaged equipment appropriately. Process EOL, defective, and/or damaged equipment through the Defense Reutilization Management Office (DRMO).

C.5.8 TASK 8 – SURGE SUPPORT (OPTIONAL)

The contractor shall provide surge support to the requirements in Tasks 1-4 and 6-7 of the awarded TO as required by unforeseen events. DCSA operates in a dynamic and evolving mission environment. It is anticipated that as a result of such an environment, augmentation of existing resources may be required in response to mission demands. For example, the unforeseen, transfer, transition, transformation to DCSA's responsibilities, consolidation of work sites or stand up of new work sites, etc. Support may require short-term Temporary Duty (TDY) (e.g., one month) or longer-term deployments (e.g., more than one month). Requirements and deliverables for the additional support are described in Tasks 1-4 and 6-7 and are within the scope of this TO but require additional personnel to meet the requirement. When additional support is needed, the Government will exercise the optional surge support CLIN.

The contractor shall develop a Surge Plan prior to the Government exercising the surge task (**Section F, Deliverable 141, Surge Plan)**. The Surge Plan shall include the project approach, milestones and schedules, major and minor deliverables, and detailed resource and cost information. The contractor shall use industry best practices and subject matter expertise to execute surge-related projects. All surge efforts shall be approved by the Government prior to start. The contractor shall staff surge resources within 30 days of formal written approval of the Surge Plan.